USER MANUAL

IMG4xxx Integrated Management Gateway

IM42xx Infrastructure Manager

CM4xxx Console Server

User Manual

Rev: 3.1

January 28th, 2008

INDEX

APPENDIX

A. Linux Commands

B. Hardware Specification

C. Safety and Certifications

D. Connectivity and Serial I/O

E. Hardware Test

F. Terminology

G. End User License Agreement

H. Service and Warranty

Chapter 1 Introduction

This Manual

This Users Manual walks you through installing and configuring your Integrated Management Gateway (IMG4004-5, IMG4216-25-DAC, IMG4216-25-DDC) Infrastructure Manager (IM4248-2-DAC, IM4248-2-DDC, IM4216-2-DAC, IM4216-2-DDC) or Console Server (CM4001, CM4008, CM4116-SAC, CM4116-SDC, CM4148-SAC, CM4148-SDC). These products are referred to generically in this manual as *IMG/IM/CM4000* or *gateway*.

Once configured, you will be able to use your IMG/IM/CM4000 to securely control your computers, as well as the firewalls, networked devices, telecommunications equipment and power strips in your data center or communications center; and securely manage similar devices in remote sites. This manual guides you in managing this infrastructure locally (across your operations or management LAN or through the local console port), and remotely (across the Internet, private network or via dial up).

Manual Organization

This manual contains the following chapters:

1. Introduction	An overview the features IMG/IM/CM4000 gateway and information on this manual
2. Installation	Physical installation of the gateway and the interconnecting of controlled devices
3. System Configuration	Describes the initial installation and configuration using the Management Console. Covers configuration of the gateway on the network and the services that will be supported
4. Serial & Network	Covers configuring serial ports and connected network hosts, and setting up User access
5. Failover and OoB dial-in	Describes setting up the high availability access features of the gateway

6. Secure Tunneling (SDT)	Covers secure remote access using SSH and configuring for RDP, VNC, HTTP, HTTPS etc access to network and serially connected devices
7. Alerts and Logging	Explains the setting up of local and remote event/ data logs and triggering SNMP and email alerts
8. Power Control	Local and remote power control of serial and network attached power strips and UPS supplies, and IPMI power control of servers
9. Authentication	All access to the gateway requires usernames and passwords which are locally or externally authenticated
10. Nagios Integration	Configuring the gateway as a distributed Nagios server
11. System Management	Covers access to and configuration of services to be run on the gateway
12. Status Reports	View the status and logs
13. Management	Includes port controls and reports that can accessed by Users
14 Basic Configuration	Command line installation and configuration using the *config* command
15. Advanced Config	More advanced command line configuration activities where you will need to use Linux commands

The latest update of this manual can be found online at
www.opengear.com/download.html

Types of users

The IMG/IM/CM4000 gateway supports two classes of users:

I. Firstly there are those users who will be authorized to configure and control the gateway; and to access and control all the connected devices. These administrative users will be set up as members of the **admin** user group and any user in this class is referred to generically in this manual as the ***Administrator***. So the Administrator can access and control the gateway using the *config* utility, the Linux command line or the browser based Management Console. By default the Administrator has access to all services and ports to control all the serial connected devices and network connected devices (*hosts*).

II. The second class of users embraces users who have been set up by the Administrator with specific limits of their access and control authority. These users are set up as members of the **users** user group (or some other user groups the Administrator may have added). They and are authorized to perform specified controls on specific connected devices are referred to as ***Users***. These Users (when authorized) can access serial or network connected devices; and control these devices using the specified services (e.g. Telnet, HHTPS, RDP, IPMI, Serial over LAN, Power Control). An authorized User can also use the Management Console to access configured devices and review port logs.

In this manual, when the term ***user*** (lower case) is used, it is referring to both the above classes of users. This document also uses the term ***remote users*** to describe users who are not on the same LAN segment as the gateway. These remote users may be Users, who are on the road connecting over the public Internet, or it may be an Administrator in another office connecting over the enterprise VPN. Also the remote users may be in the same room or the same office but connected on a separate VLAN to the gateway.

Management Console

The IMG/IM/CM4000 Management Console runs in a browser and provides a view of the gateway and all the connected equipment. Administrators can use the Management Console, either locally or from a remote location, to configure the gateway, the Users and the ports and connected hosts.

An authorized User can then use the Management Console to access and control configured devices, review port logs, use the in-built java terminal to access serially attached console and control power to connected devices.

The Management Console is accessed through the IP Network or through a modem/ ISDN connection.

The IMG/IM/CM4000 runs an embedded Linux operating system, and experienced Linux and UNIX users may prefer to undertake configuration at the command line. You can get command line access by connecting through a terminal emulator or communications program to the console serial port; by ssh or telnet connecting through the LAN; or through an SSH tunneling to the gateway.

Manual Conventions

This manual uses different fonts and typefaces to show specific actions:

> **Note** Text presented like this indicates issues to take note of.

> ***WARNING***
> ***Text presented like this highlights important issues.***
> ***It is essential you read and take head of these warnings.***

- Text presented with an arrow head indent indicates an action you should take as part of the procedure.

Bold text indicates text that you type, or the name of a screen object (*e.g.* a menu or button) on the Management Console.

Italic text is also used to indicate a text command to be entered at the command line level.

Chapter 2 Installation

Introduction

This chapter describes the physical installation of the IMG/IM/CM4000 hardware and interconnection to the network and controlled appliances.

WARNING
To avoid physical and electrical hazard
please read Appendix C on Safety

2.1 Models

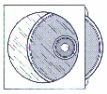
There are multiple IMG/IM/CM4000 models each with a different number of network and serial ports or power supply:

	Serial Ports	Network Ports	Console Port	Modem	Power
IM4248-2-DAC	48	2	1	Internal	Dual AC Universal Input
IM4248-2-DDC	48	2	1	Internal	Dual DC Universal Input
IM4216-2-DAC	16	2	1	Internal	Dual AC Universal Input
IM4216-2-DDC	16	2	1	Internal	Dual DC Universal Input
IM4208-2-DAC	8	2	1	Internal	Dual AC Universal Input
IM4208-2-DDC	8	2	1	Internal	Dual DC Universal Input
IMG4216-25-DAC	16	25	1	Optional	Dual AC Universal Input
IMG4216-25-DDC	16	25	1	Optional	Dual DC Universal Input
IMG4004-5	4	5	1	Optional	External AC/DC adapter
CM4148-SAC	48	1	1		Single AC Universal Input
CM4148-SDC	48	1	1		Single 48 VDC Input
CM4116-SAC	16	1	1		Single AC Universal Input
CM4116-SDC	16	1	1		Single 48 VDC Input
CM4008	8	1	1		External AC/DC adapter

CM4001	1	1	1	External AC/DC adapter

The tables below show the components shipped with each model.

2.1.1 IM4208-2, IM4216-2, IM4248-2 and IMG4216-25 Kit Components

	Part # 509006 (509007) or Part # 50908	IM4216-2 (IM4248-2 or IM4208-2) Infrastructure Manager or IMG4216-25 Management Gateway
	Part # 440016	2 x Cable UTP Cat5 blue
	Part # 319000 and 319001	Connector DB9F-RJ45S straight and DB9F-RJ45S cross-over
	Part # 440001	Dual IEC AC power cord (DAC models only)
	Part # 539001	Quick Start Guide and CD-ROM

- Unpack your IM/IMG42xx (IM4208-2, IM4216-2, IM4248-2 Infrastructure Manager or IM4216-25 Management Gateway) kit and verify you have all the parts shown above, and that they all appear in good working order
- If you are installing your IM/IMG42xx in a rack you will need to attach the rack mounting brackets supplied with the unit, and install the unit in the rack. Take care to head the Safety Precautions listed in Appendix C
- Proceed to connect your IM/IMG42xx to the network, to the serial ports of the controlled devices, and to power as outlined below

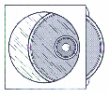
2.1.2 IMG4004-5 Kit Components

	Part # 509010	IMG4004-5 Management Gateway

Part # 440016 2 x Cable UTP Cat5 blue

Part # 319000 and 319001 Connector DB9F-RJ45S straight and DB9F-RJ45S cross-over

Part # 450006 and 440001 Power Supply 5VDC 2.0A IEC Socket and AC power cable



Part #539000 Quick Start Guide and CD-ROM

- Unpack your IMG4004-5 kit and verify you have all the parts shown above, and that they all appear in good working order
- Proceed to connect your IMG4004-5 to the network, the serial ports and LAN ports of the controlled devices and to the AC power as shown below

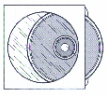
2.1.3 CM4116 or CM4148 Kit Components

Part # 509001 (or Part # 509002) CM4116 (CM4148) Console Server

Part # 440016 2 x Cable UTP Cat5 blue

Part # 319000 and 319001 Connector DB9F-RJ45S straight and DB9F-RJ45S cross-over

Part # 440001 IEC AC power cord (SAC model only)



Part # 539001 Quick Start Guide and CD-ROM

- Unpack your CM4116 (or CM4148) kit and verify you have all the parts shown above, and that they all appear in good working order

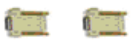
- If you are installing your CM4116 (or CM4148) in a rack you will need to attach the rack mounting brackets supplied with the unit, and install the unit in the rack. Take care to head the Safety Precautions listed in Appendix C
- Proceed to connect your CM4116 (or CM4148) to the network, to the serial ports of the controlled devices, and to power as outlined below

Note The CM4116-SDC and CM4148-SDC products are DC powered and the Kits do not include an IEC AC power cord.

2.1.4 CM4008 Kit Components

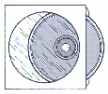
Part # 509000 CM4008 Console Server

Part # 440016 2 x Cable UTP Cat5 blue



Part # 319000 and 319001 Connector DB9F-RJ45S straight and DB9F-RJ45S cross-over

Part # 450006 and 440001 Power Supply 5VDC 2.0A IEC Socket and AC power cable



Part #539000 Quick Start Guide and CD-ROM

- Unpack your CM4008 kit and verify you have all the parts shown above, and that they all appear in good working order
- Proceed to connect your CM4008 to the network, the serial ports of the controlled servers and AC power as shown below

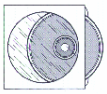
2.1.5 CM4001 Kit Components

Part # 509003 CM4001 Console Server

Part # 440016 2 x Cable UTP Cat5 blue

Part # 319000 and 319001 Connector DB9F-RJ45S straight and DB9F-RJ45S cross-over

Part # 4500XX Power Supply 12VDC 1.0A Wall mount



Part #539000 Quick Start Guide and CD-ROM

- Unpack your CM4001 and verify you have all the parts shown above, and that they all appear in good working order
- Proceed to connect your CM4001 to the network, to the serial ports of the controlled devices, and to power as outlined below

2.2 Power connection

2.2.1 IMG4216-25-DAC, IM4208-2-DAC, IM4216-2-DAC and IM4248-2-DAC Power

The IM42XX and IMG4216-25 gateways all have dual universal AC power supplies with auto failover built in. These power supplies each accept AC input voltage between 100 and 240 VAC with a frequency of 50 or 60 Hz and the total power consumption per gateway is less than 30W. Two IEC AC power sockets are located at the rear of the metal case, and these IEC power inlets use conventional IEC AC power cords. Power cords for various regions are available, although the North American power cord is provided by default. There is a warning notice printed on the back of each unit:

WARNING
To avoid electrical shock the power cord grounding conductor must be connected to ground.

2.2.2 CM4116-SAC and CM4148-SAC Power

The CM4116 and CM4148 models have a built-in universal auto-switching AC power supply. This power supply accepts AC input voltage between 100 and 240 VAC with a frequency of 50 or 60 Hz and the power consumption is less than 20W.

Both CM4116 and CM4148 models have an IEC AC power socket located at the rear of the metal case. This IEC power inlet uses a conventional IEC AC power cord, and the power cords for various regions are available. (The North American power cord is provided by default). There is a warning notice printed on the back of each unit:

WARNING
To avoid electrical shock the power cord grounding conductor must be connected to ground.

2.2.3 IMG4004-5 and CM4008 Power

The IMG4004-5 and CM4008 are supplied with an external DC power supply unit. This unit accepts an AC input voltage between 100 and 250 VAC with a frequency of 50Hz or 60Hz. The DC power supply has an IEC AC power socket, which accepts a conventional IEC AC power cord. The power cord for North American is provided by default. The 5V DC connector from the power supply plugs into the 5VDC power socket on the rear of the IMG4004-5 or CM4008 chassis.

2.2.4 CM4001 Power

The CM4001 is supplied with an external DC wall mount power supply unit. Specific units are supplied for North American, Europe, UK, Japan and Australia. The 12V DC connector from the power supply unit plugs into the 9V-12VDC power socket on the rear of the CM4001 chassis.

- Plug in the AC power cable (and the DC power cable for CM4001/4008) and turn AC power On
- Confirm the Power LED on the CM4000 is lit. (Note: When you have applied power to the CM4008, you will also observe the LEDs P1 through P8 light up in sequence. On the CM4001 you will observe the Local and Serial LEDs flashing alternately)

2.2.5 CM4116-SDC and CM4148-SDC Power

The CM4116-SDC and CM4148-SDC models have a DC power connector block located at the rear of the metal case:

WARNING

You must connect the CM41xx-SDC only to a DC-input power source that has an input supply voltage from 36 to 72 VDC. If the supply voltage is not in this range, the console server might not operate properly or might be damaged.

You can identify the positive and negative feed positions from the label on the four way screw terminal block:

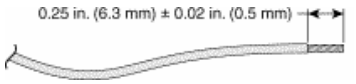
+	E	E	-

The '**+**' Terminal on the four way screw terminal block should always be connect to the more positive voltage (from 0V to +48 V)

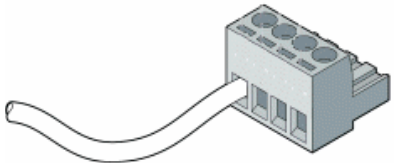
The '**-**' terminal on the four way screw terminal block should connect to the more negative voltage (from -48V to 0V)

The CM41xx-SDC is a floating (wrt Earth), however there are two '**E**' terminals on the four way screw terminal block which are Earth or Chassis Ground

It is recommended that 18-gauge copper wire be used to connect to the DC-power source. Strip each of the wires to 0.25inch (6.6 mm) (stripping more than this can leave exposed wire from the terminal block plug after installation):



Insert the exposed wire of each of the DC-input power source wires into the terminal block plug, making sure that you cannot see any wire lead, and tighten the terminal block captive screw:



Insert the terminal block plug in the terminal block header on the rear panel of the CM41xx-SDC:

2.2.6 IMG4216-25-DDC, IM4208-2-DDC, IM4216-2-DDC and IM4248-2-DDC Power

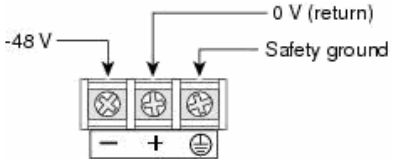
The IM42XX and IMG4216-25 DDC gateways all have dual DC power supplies with auto failover built in. To connect to the DC input supply:

- Strip the DC wire insulation to expose approximately 0.4 inch (10 mm) of conductor
- Connect the safety ground wire to the '**E**' safety ground terminal on the terminal block first. The DDC is floating (wrt Earth), however the safety terminal on the three way screw terminal block connects to Earth or Chassis Ground
- Connect the power wires to the appropriate terminals of the terminal block:

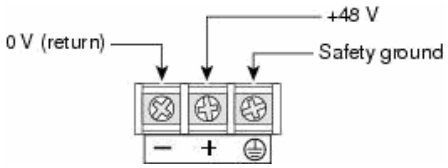
  The '**+**' Terminal on the four way screw terminal block should always be connect to the more positive voltage (from 0V to +48 V)

  The '**-**' terminal on the four way screw terminal block should connect to the more negative voltage (from -48V to 0V)

  So the connections for -48 Volt DC input power are:



  The connections for -48 Volt DC input power are:



- Tighten the terminal screw to a torque of 8.0 ± 0.5 in-lb (0.93 ± 0.05 N-m)
- Repeat the connection steps above for the second power supply
- Turn on the DC power

WARNING

The safety covers are an integral part of the DDC product. Do not operate the unit without the safety cover installed.

Also any exposed wire lead from a DC-input power source can conduct harmful levels of electricity. So ensure that no exposed portion of the DC-input power source wire extends from the terminal block plug and safety cover.

2.3 Network connection

The RJ45 LAN ports are located on the rear panel of the CM4001/4008, and on the front panel of the rack-mount CM41xx and IM/IMG42xx. All physical connections are made using industry standard Cat5 cabling and connectors. Ensure you only connect the LAN port to an Ethernet network that supports 10Base-T/100Base-T. For the initial configuration of the IMG/IM/CM4000 you must connect a PC or workstation to the gateway's principal network port (which is labeled *NETWORK* on IMG4xxx, *NETWORK1* on IM42xx and *LAN* on CM4xxx gateways)

2.4 Serial Port connection

The RJ45 serial ports are located on the rear panel of the IMG4004-5 and CM4008; and on the front panel of the rack mount IMG4216-25, CM41xx and IM42xx. The CM4001 has a DB9 serial port connector. All devices have a DB9 LOCAL (Console/Modem) port which is on the rear of the CM4001/4008 and the front of the CM41xx and IM/IMG42xx.

Conventional Cat5 cabling with RJ45 jacks are used for serial connections. Before connecting the console port of an external device to the IMG/IM/CM4000 serial port, confirm that the device does support the standard RS-232C (EIA-232).

Opengear supplies an extensive range of cables and adapters that may be required to connect to the more popular servers and network appliances. These are overviewed in Appendix D (Connectivity and Serial I/O). More detailed information is available online at http://www.opengear.com/cabling.html

Note Care should be taken in handling IMG/IM/CM4000 products. There are no operator serviceable components inside, so please do not remove covers, and do refer service to qualified personnel.

Chapter 3 Initial System Configuration

Introduction

This chapter provides step-by-step instructions for the initial configuration of your IMG/IM/CM4000 gateway, and connecting it to the Management or Operational LAN. This involves the Administrator:

- Accessing the Management Console
- Changing the Administrator password
- Setting the IP address gateway's principal LAN port
- Selecting the network services to be supported

This chapter also discusses the communications software tools that the Administrator may use in accessing the gateway, and configuring of the other LAN ports on the IM/IMG42xx.

3.1 Management console connection

Your IMG/IM/CM4000 comes configured with a default IP Address 192.168.0.1 Subnet Mask 255.255.255.0

- Directly connect a PC or workstation to the IMG/IM/CM4000

Note For initial configuration it is recommended that the IMG/IM/CM4000 be connected directly to a single PC or workstation. However, if you choose to connect your LAN before completing the initial setup steps, it is important that:

- you ensure there are no other devices on the LAN with an **address of 192.168.0.1**
- the console server and the PC/workstation are on the same LAN segment, with no interposed router appliances

To configure the IMG/IM/CM4000 with a browser, the connected PC or workstation should have an IP address in the same range as the IMG/IM/CM4000 (e.g. 192.168.0.100):

- To configure the IP Address of your Linux or Unix PC/workstation simply run *ifconfig*

- For Windows PCs (Win9x/Me/2000/XP/ NT):

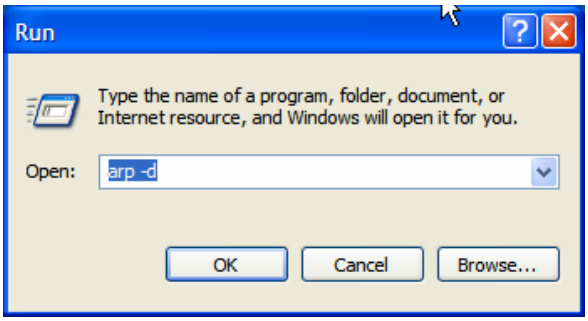
  - Click **Start** -> (**Settings** ->) **Control Panel** and double click **Network Connections** (for 95/98/Me, double click **Network**).
  - Right click on **Local Area Connection** and select **Properties**
  - Select **Internet Protocol (TCP/IP)** and click **Properties**
  - Select **Use the following IP address** and enter the following details:
    IP address: **192.168.0.100**
    Subnet mask: **255.255.255.0**
  - If you wish to retain your existing IP settings for this network connection, click **Advanced** and **Add** the above as a secondary IP connection.

If it is not convenient to change the PC/workstation network address, you can use the *ARP-Ping* command as described in the Note below to reset the IMG/IM/CM4000 IP address:

Note ARP-Ping IP Address Assignment

An alternative connection option is to use the *arp* command on a network connected PC/workstation to assign an alternate starting IP address to the IMG/IM/CM4000. To do this from a Windows PC:

- Click **S**tart -> R**un**
- Type *cmd* and click **OK** to bring up the command line
- Type *arp –d* to flush the ARP cache
- Type *arp –a* to view the current ARP cache which should be empty



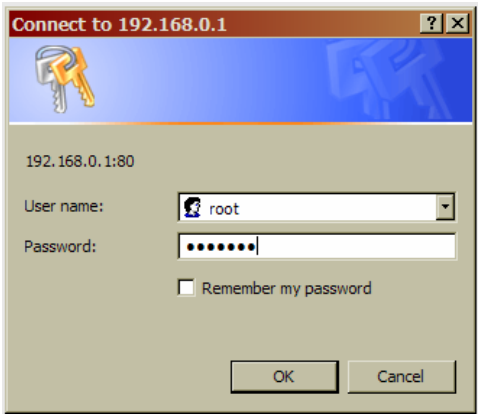
Now add a static entry to the ARP table and ping the IMG/IM/CM4000 to have it take up the IP address. In the example below we have an IMG/IM/CM4000 with a MAC Address 00:13:C6:00:02:0F (designated on the label on the bottom of the unit) and we are setting its IP address to 192.168.100.23: Also the PC/workstation issuing the *arp* command must be on the same network segment as the IMG/IM/CM4000 (i.e. have an IP address of 192.168.100.xxx).

- Type *arp -s 192.168.100.23 00-13-C6-00-02-0F*
  (Note for UNIX the syntax is:
  arp -s 192.168.100.23 00:13:C6:00:02:0F)
- Type *ping -t 192.18.100.23* to start a continuous ping to the new IP Address.
- Turn on the IMG/IM/CM4000 and wait for it to configure itself with the new IP address. It will start replying to the ping at this point
- Type *arp –d* to flush the ARP cache again

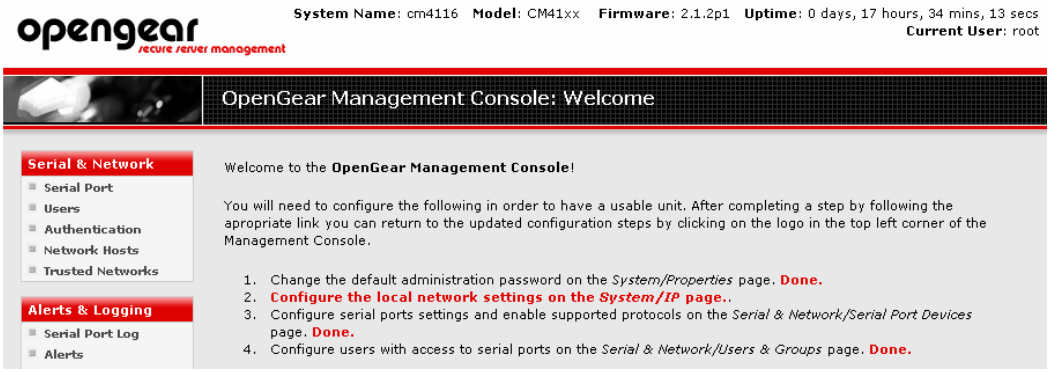
- Activate your preferred browser on the connected PC/ workstation and enter **https://192.168.0.1** The Management Console supports all current versions of the popular browsers (Netscape, Internet Explorer, Mozilla Firefox and more)

- You will be prompted to log in. Enter the default administration username and administration password:

  Username: **root**
  Password: **default**



> **Note** IMG/IM/CM4000 gateways with firmware versions later than V2.2 are factory configured with HTTP disabled and HTTPS enabled appliances



A **Welcome** screen, which lists the four basic installation configuration steps, will be displayed:

1. **Change the default administration password on the System/Administration page** (*Chapter 3*)
2. **Configure the local network settings on the System/IP page** (*Chapter 3*)
3. **Configure port settings and enable supported protocols on the Serial & Network/Serial Port page** (*Chapter 4*)
4. **Configure users with access to serial ports on the Serial & Network/Users page** (*Chapter 3*)

After completing each of the above steps, you can return to the configuration list by clicking in the top left corner of the screen on the opengear logo

As you complete each step, the configuration list will be updated *e.g.* after you have configured the serial ports it will display this step as:

3. **Configure serial ports settings and enable supported protocols on the Serial & Network/Serial Port Devices page Done.**

Note If you are not able to connect to the Management Console at 192.168.0.1 or if the default Username / Password were not accepted then reset your IMG/IM/CM4000 (refer *Chapter 10*)

3.2 Administrator Password

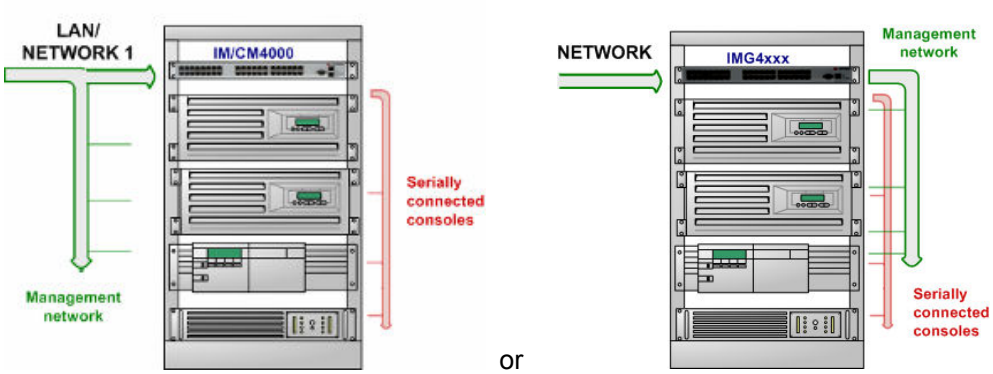
For security reasons, only the Administrator (the administration user named **root)** can initially log into your gateway. So only those people who know the root password can access and reconfigure the IMG/IM/CM4000 gateway itself. The corollary is that anyone who correctly guesses the root password could gain access (and the default root password is **default**). So it is important that you enter and confirm a new password before giving the IMG/IM/CM4000 any access to, or control of, your computers and network appliances.

- Select **System: Administration**
- Enter a new **System Password** then re-enter it in **Confirm System Password.** This is the new password for **root**, the main administrative user account, so it is important that you choose a complex password, and keep it safe
- At this stage you may also wish to enter a **System Name** and **System Description** for the IMG/IM/CM4000 gateway to give it a unique ID and make it simple to identify
- Click **Apply**. As you have changed the password you will be prompted to log in again. This time use the new password

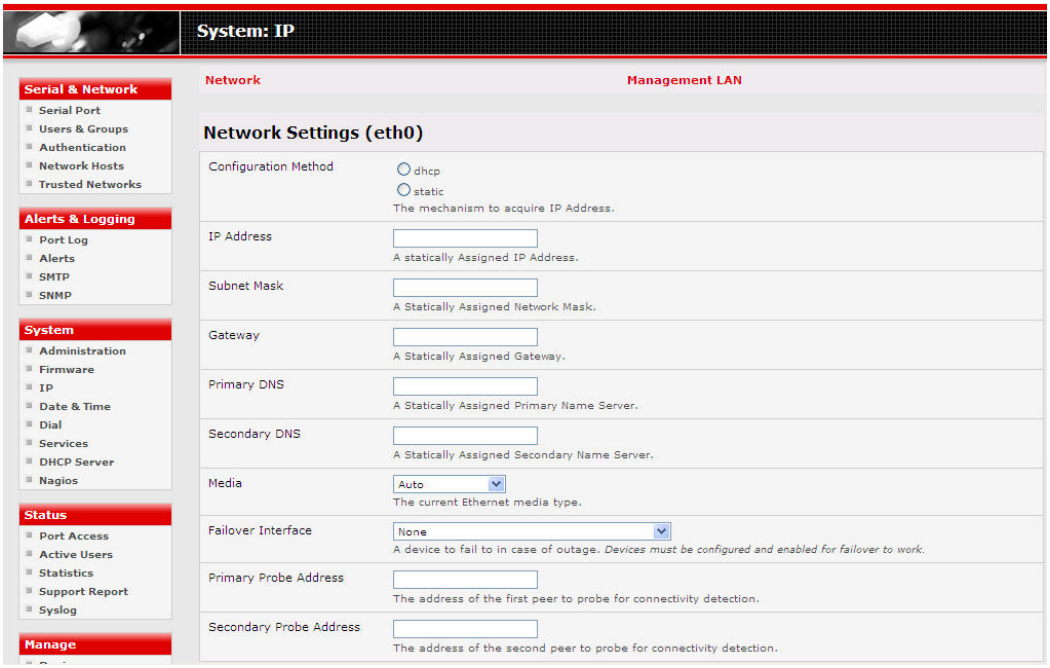
Note If you are not confident your IMG/IM/CM4000 has been supplied with the current release of firmware, you can upgrade. Refer *Upgrade Firmware - Chapter 10*

3.3 Network IP address

You now must enter an IP address for the principal Ethernet (*LAN/Network/Network1*) port on the IMG/IM/CM4000 gateway; or enable its DHCP client so that it automatically obtains an IP address from a DHCP server on the network it is to be connected to.



- On the **System: IP** menu select the **Network** page then check **dhcp** or **static** for the **Configuration Method**
- If you selected **static** you must manually enter the new **IP Address**, **Subnet Mask**, **Gateway** and **DNS** server details. This selection automatically disables the DHCP client



- If you selected **dhcp** the IMG/IM/CM4000 will look for configuration details from a DHCP server on your management LAN. This selection automatically disables any static address. The IMG/IM/CM4000 MAC address can be found on a label on the base plate

> **Note** In its factory default state (with no Configuration Method selected) the IMG/IM/CM4000 has its DHCP client enabled, so it automatically accepts any network IP address assigned by a DHCP server on your network. In this initial state, the IMG/IM/CM4000 will then respond to both its Static address (192.168.0.1) and its newly assigned DHCP address.

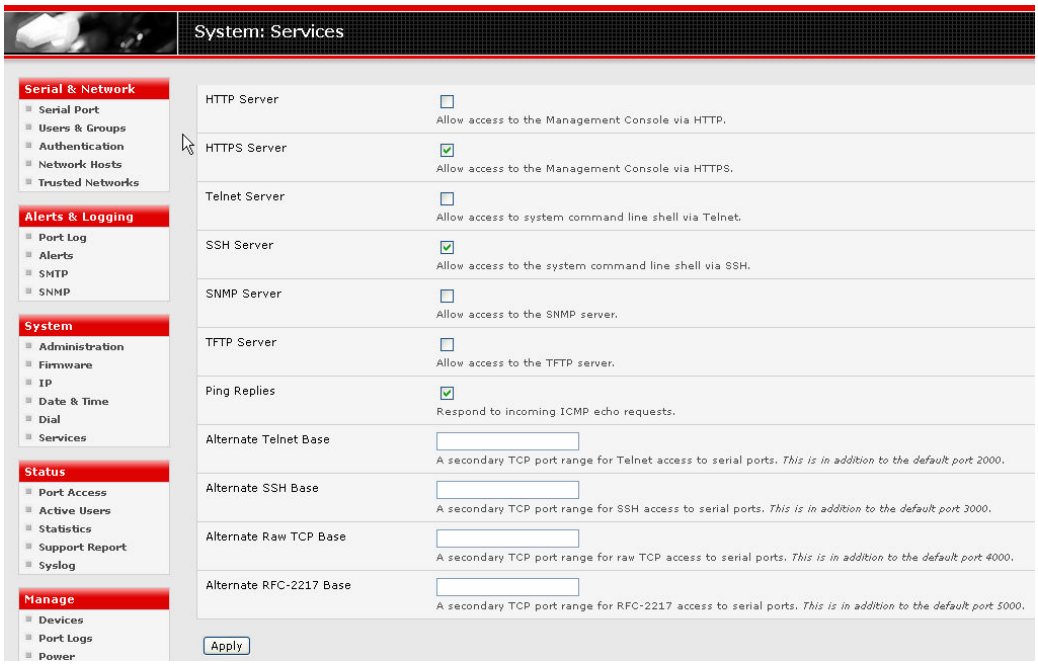
- By default the IMG/IM/CM4000 LAN port auto detects the Ethernet connection speed. However you can use the **Media** menu to lock the Ethernet to 10 Mb/s or 100Mb/s and to Full Duplex (FD) or Half Duplex (HD)

> **Note** If you have changed the IM/CM4000 IP address, you may need to reconfigure your PC/workstation so it has an IP address that is in the same network range as this new address (as detailed in an earlier note in this chapter).

- Click **Apply**
- You will need to reconnect the browser on the PC/workstation that is connected to the IMG/IM/CM4000 by entering **http://new IP address**

3.4 System Services

The Administrator can access and configure the IMG/IM/CM4000 gateway using a range of access protocols. The factory default enables HTTPS and SSH access and disables HTTP and Telnet. The factory default for gateways pre firmware version 2.2 enabled HTTP, HTTPS, Telnet and SSH. The Administrator can simply disable any of the services, or enable others:



- Select the **System: Services** option then select /deselect for the service to be enabled /disabled. The following access protocol options are available:

HTTPS This ensures secure browser access to all the Management Console menus. It also allows appropriately configured Users secure browser access to selected Management Console *Manage* menus. If you enable HTTPS, the Administrator will be able to use a secure browser connection to the IMG/IM/CM4000 gateway's Management Console. For information on certificate and user client software configuration refer *Chapter 9 - Authentication*. By default HTTPS is enabled, and it is recommended that only HTTPS access be used if the gateway is to be managed over any public network (e.g. the Internet).

HTTP The HTTP service allows the Administrator basic browser access to the Management Console. It is recommended the HTTP service be disabled if the IMG/IM/CM4000 gateway is to be remotely accessed over the Internet.

Telnet This gives the Administrator telnet access to the system command line shell (Linux commands). While this may be suitable for a local direct connection over a management LAN, it is recommended this service be disabled if the IMG/IM/CM4000 is to be remotely administered.

SSH This service provides secure SSH access to the Linux command line shell. It is recommended you choose SSH as the protocol where the Administrator connects to the gateway over the Internet or any other public network. This will provide authenticated communications between the SSH client program on the remote PC/workstation and the SSH sever in the gateway. For more information on SSH configuration refer *Chapter 9 - Authentication*.

- There are also a number of related service options that can be configured at this stage:

SNMP This will enable *netsnmp* in the gateway, which will keep a remote log of all posted information. SNMP is disabled by default. To modify these default SNMP settings, the Administrator must make the edits at the command line as described in *Chapter 15 – Advanced Configuration*

TFTP This is relevant to IM42xx and IMG4xxx gateways only as it will set up default *tftp* server on the USB flash card. This server can be used to store config files, maintain access and transaction logs etc

Ping This allows the IMG/IM/CM4000 to respond to incoming ICMP echo requests. Ping is enabled by default, however for security reasons this service should generally be disabled post initial configuration

- And there are some serial port access parameters that can be configured on this menu:

Base The IMG/IM/CM4000 uses specific default ranges for the TCP/IP ports for the various access services that Users and Administrators can use to access devices attached to serial ports (as covered in *Chapter 4 – Configuring Serial Ports*). The Administrator can also set alternate ranges for these services, and these secondary ports will then be used in addition to the defaults.

The default TCP/IP **base** port address for *telnet* access is 2000, and the range for *telnet* is IP Address: Port (2000 + serial port #) *i.e.* 2001 – 2048. So if the Administrator were to set 8000 as a secondary base for telnet then serial port #2 on the gateway can be telnet accessed at IP Address:2002 and at IP Address:8002.

The default base for SSH is 3000; for Raw TCP is 4000; and for RFC2217 it is 5000

- Click **Apply**. As you apply your services selections, the screen will be updated with a confirmation message:

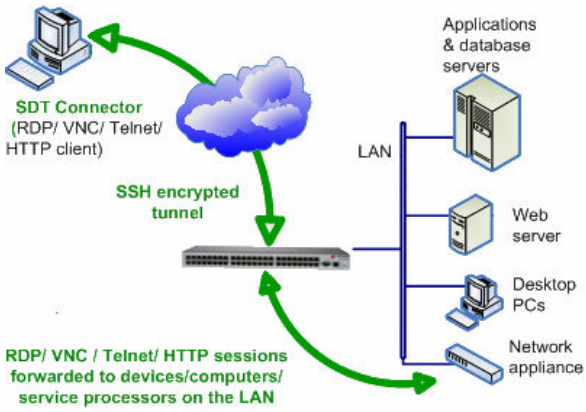
  Message Changes to configuration succeeded.

3.5 Communications Software

You have configured access protocols for the Administrator client to use when connecting to the IMG/IM/CM4000. User clients (who you may set up later) will also use these protocols when accessing IMG/IM/CM4000 serial attached devices and network attached hosts. So you will need to have appropriate communications software tools set up on the Administrator (and User) client's PC/workstation. Opengear provides the *SDTConnector* as the recommended client software tool, however other generic tools such as PuTTY and SSHTerm may be used, and these are all described below:

3.5.1 SDTConnector

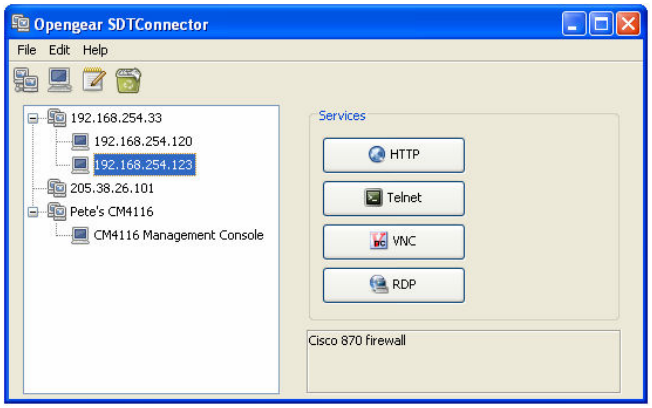
Opengear recommends using the *SDTConnector* communications software tool for all communications with IMG/IM/CM4000 gateways, to ensure these communications are secure. Each IMG/IM/CM4000 is supplied with an unlimited number of *SDTConnector* licenses to use with that gateway.



SDTConnector is a light weight tool that enables Users and Administrators to securely access the IMG/IM/CM4000 gateway, and the various computers, network devices and appliances that may be serially or network connected to the gateway.

SDTConnector is a Java client program that couples the trusted SSH tunneling protocol with popular access tools such as Telnet, SSH, HTTP, HTTPS, VNC, RDP to provide point-and-click secure remote management access to all the systems and devices being managed.

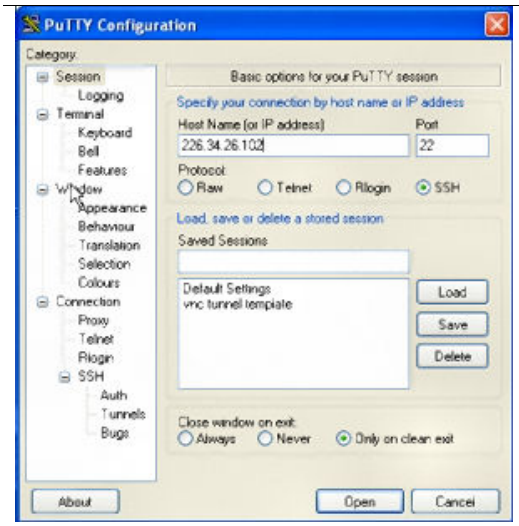
Information on using *SDTConnector* for browser access to the gateway's Management Console, Telnet/SSH access to the gateway command line, and TCP/UDP connecting to hosts that are network connected to the gateway can be found in *Chapter 6 - Secure Tunneling.*



SDTConnector can be installed on Windows 2000, XP, 2003, Vista PCs and on most Linux, UNIX and Solaris. For full information on installing, configuring and using *SDTConnector* refer to the **SDTConnector User Manual** on the IMG/IM/CM4000 CD (or online at *ftp://ftp.opengear.com/manual/*)

3.5.2 PuTTY

Communications packages like *PuTTY* can be also used to connect to the IMG/IM/CM4000 gateway command line (and to connect serially attached devices as covered in *Chapter 4*). *PuTTY* is a freeware implementation of Telnet and SSH for Win32 and UNIX platforms. It runs as an executable application without needing to be installed onto your system. *PuTTY* (the Telnet and SSH client itself) can be downloaded at http://www.tucows.com/preview/195286.html

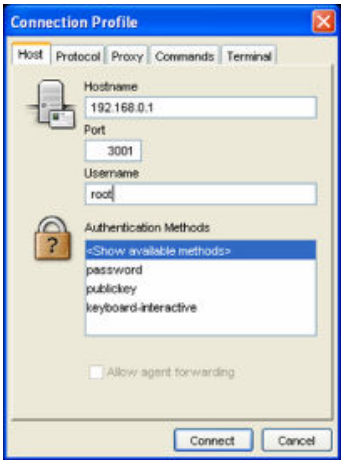


- To use PuTTY for an SSH terminal session from a Windows client, you enter the gateway's IP address as the 'Host Name (or IP address)'
- To access the IMG/IM/CM4000 command line you select 'SSH' as the protocol, and use the default IP Port 22
- Click 'Open' and you will be presented with the IMG/IM/CM4000 login prompt. (You may also receive a 'Security Alert' that the host's key is not cached, you will need to choose 'yes' to continue.)
- Using the Telnet protocol is similarly simple - but you use the default port 23

3.5.3 SSHTerm

Another common communications package that may be useful is *SSHTerm,* an open source package that can be downloaded from http://sourceforge.net/projects/sshtools

- To use *SSHTerm* for an SSH terminal session from a Windows Client you simply Select the 'File' option and click on 'New Connection'.
- A new dialog box will appear for your 'Connection Profile' where you can type in the host name or IP address (for the IMG/IM/CM4000 unit) and the TCP port that the SSH session will use (port 22). Then type in your username and choose password authentication and click connect.



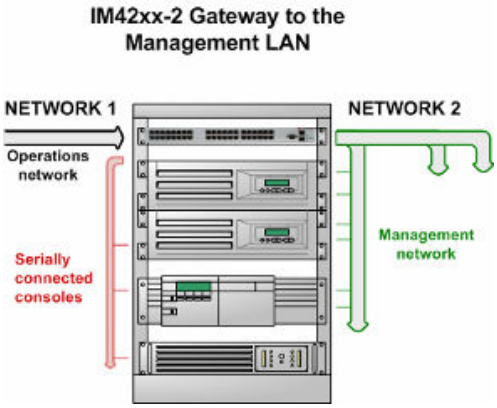
- You may receive a message about the host key fingerprint, and you will need to select 'yes' or 'always' to continue.
- The next step is password authentication and you will be prompted for your username and password from the remote system. You will then be logged on to the IMG/IM/CM4000 gateway

3.6 Management network configuration (IM42xx & IMG4xxx only)

The IMG4xxx and IM42xx gateways have additional Ethernet network ports that can be configured as a management gateway/ LAN port or as a failover/ OOB access port.

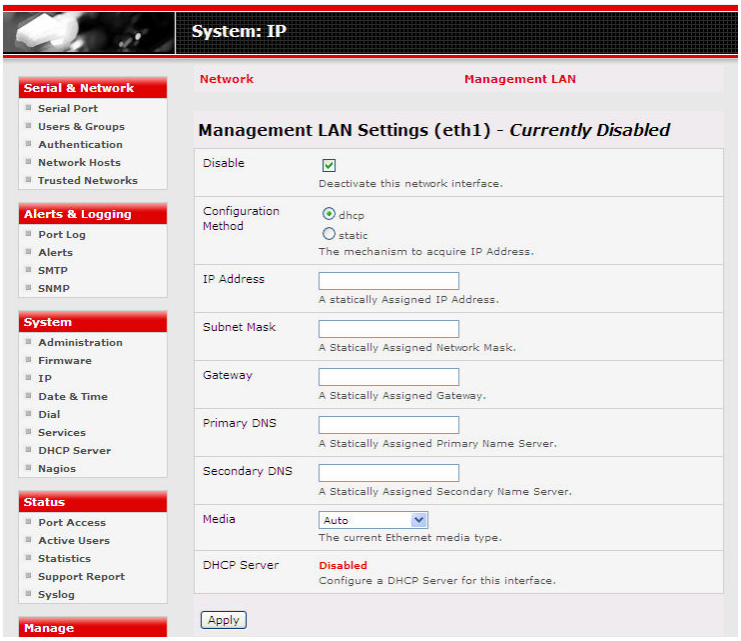
3.6.1 Enable the Management LAN gateway

The IMG4xxx and IM42xx provide a management LAN gateway with firewall, router and DHCP server. With an IM42xx you will need to connect an external LAN switch to *Network 2* to attach hosts to the management LAN. Whereas the IMG4xxx has an integrated four or twenty four port management LAN switch (i.e. it provides a firewall, router, DHCP server and VLAN switch).



However these features are all disabled by default. To configure the Management LAN gateway:

- Select the **Management LAN** page on the **System: IP** menu and uncheck **Disable**
- Configure the **IP Address** and **Subnet Mask** for the Management LAN (leaving the **Gateway** and **DNS** fields blank) then click **Apply**



Note The IMG4xxx can be configured with an active Management LAN/gateway **and** with one of the switched Ethernet ports configured for OOB/Failover (ETH 4 on the IMG4004-5 or ETH 24 on the IMG4216-25).

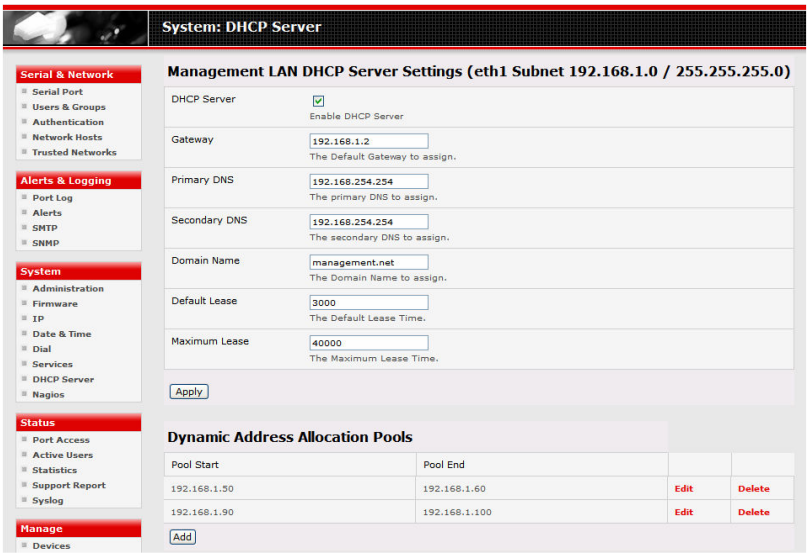
With the IM42xx, the second Ethernet port can be configured as either a gateway port **or** it can be configured as an OOB/Failover port - but not both. So ensure you did not allocate **Network 2** as the **Failover Interface** when you configured the IM42xx's principal **Network** connection on the **System: IP** menu.

The management gateway function is now enabled with default firewall and router rules. These rules can be reconfigured at the command line. The IMG4xxx and IM42xx gateways also host a DHCP server, which by default is disabled.

3.6.2 Configure the Management LAN DHCP server

The DHCP server enables the automatic distribution of IP addresses to hosts running DHCP clients on the Management LAN. To enable the DHCP server:

- On the **System: IP** menu select the **Management LAN** page and click the **Disabled** label in the **DHCP Server** field; or go to the **System: DHCP Server** menu and check **Enable DHCP Server**



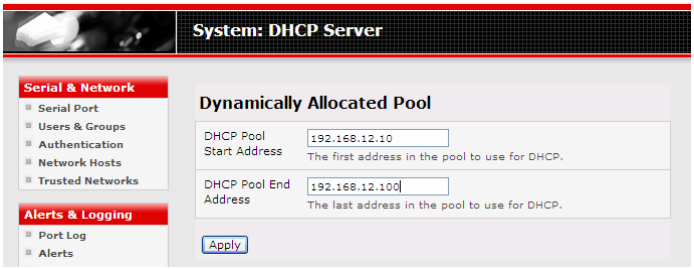
To configure the DHCP server for the Management LAN:

- Enter the **Gateway** address that is to be issued to the DHCP clients. If this field is left blank, the IMG/IM4xxx unit's IP address will be used
- Enter the **Primary DNS** and **Secondary DNS** address to issue the DHCP clients. Again if this field is left blank, the IMG/IM4xxx unit's IP address is used, so leave this field blank for automatic DNS server assignment
- Optionally enter a **Domain Name** suffix to issue DHCP clients

- Enter the **Default Lease** time and **Maximum Lease** time in seconds. The lease time is the time that a dynamically assigned IP address is valid before the client must request it again
- Click **Apply**

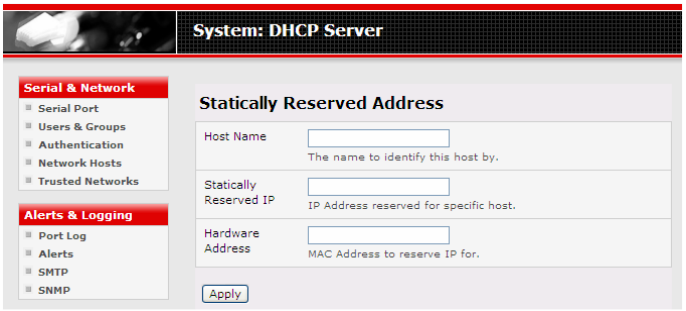
The DHCP server will sequentially issue IP addresses from a specified address pool(s):

- Click **Add** in the **Dynamic Address Allocation Pools** field
- Enter the **DHCP Pool Start Address** and **End Address** and click **Apply**



The DHCP server also supports pre-assigning IP addresses to be allocated only to specific MAC addresses and reserving IP addresses to be used by connected hosts with fixed IP addresses. To reserve an IP addresses for a particular host:

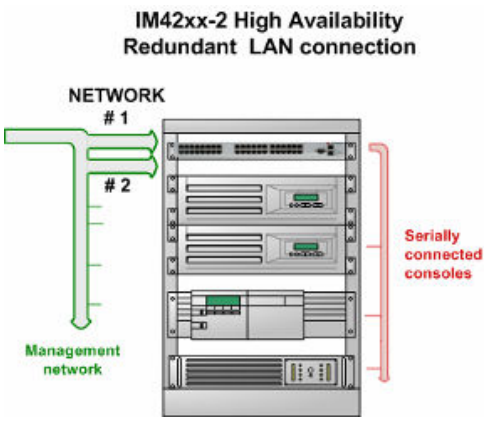
- Click **Add** in the **Reserved Addresses** field
- Enter the **Hostname,** the **Hardware Address** (MAC) and the **Statically Reserved IP** address for the DHCP client and click **Apply**



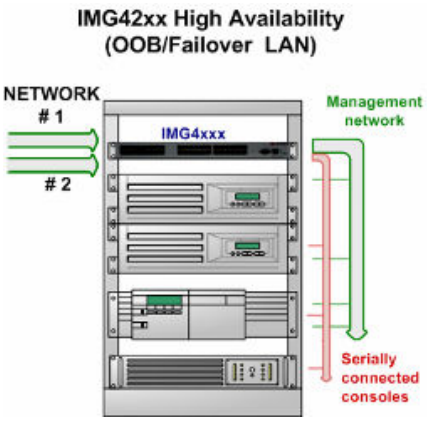
When DHCP has initially allocated hosts addresses it is recommended to copy these into the pre-assigned list so the same IP address will be reallocated in the event of a reboot.

3.6.3 Select Failover or broadband OOB

The IMG4xxx and IM42xx gateways provide a failover option so in the event of a problem using the main LAN connection for accessing the gateway; an alternate access path is used.

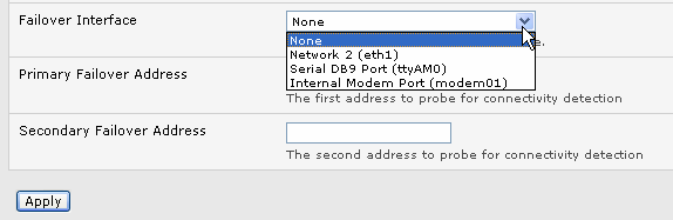


or



- By default the failover is not enabled. To enable, select the **Network** page on the **System: IP** menu

- Now select the **Failover Interface** to be used in the event of an outage on the main network. This can be:
  - an alternate broadband Ethernet connection (which would be the *Network2* port on IM42xx, or Management LAN port 4 on the IMG4004-5 or Management LAN port 24 on the IMG4216-25) or
  - the IM/IMG42xx internal modem or
  - an external serial modem/ISDN device connected to the IM/IMG42xx Console port (for out-dialing to an ISP or the remote management office)



- Click **Apply**. You have selected the failover method however it is not active until you have specified the external sites to be probed to trigger failover, and set up the failover ports themselves. This is covered in *Chapter 5*.

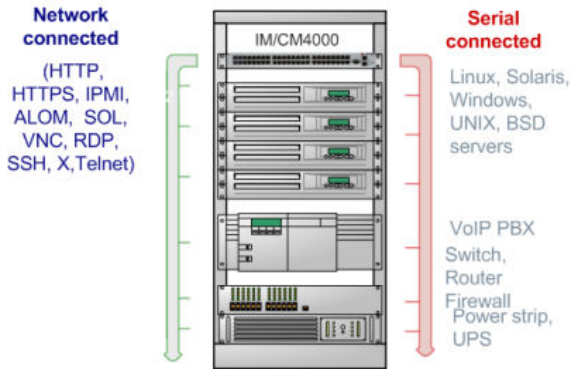
Note The IMG4xxx can be configured with an active Management LAN/gateway and with one of the switched Ethernet ports configured for OOB/Failover (Eth 4 on the IMG4004-5 or Eth 24 on the IMG4216-25).

However with the IM42xx, the second Ethernet port can be configured as either a gateway port or as an OOB/Failover port, but not both. So ensure you did not enable the Management LAN function on **Network 2**

Chapter 4 Serial Port and Network Host Configuration

Introduction

The IMG/IM/CM4000 enables access and control of serially-attached dives and network-attached devices (*hosts*). The Administrator must configure the port access privileges for each of these devices, and specify the selection of services that can be used to control the devices. The Administrator must also set up Users and specify each User's individual access and control privileges.



This chapter covers each of the steps in configuring hosts and serially attached devices:

- Configure Serial Ports – setting up the protocols to be used in accessing serially-connected devices
- Users & Groups – setting up Users and defining the access permissions for each of these Users
- Authentication – covered in more detail in *Chapter 9*
- Network Hosts – configuring access to local network connected computers or appliances (referred to as *hosts*)
- Trusted Networks
- Serial Port Redirection Client

4.1 Configuring Serial Ports

To configure the serial port you must first set the protocols and the RS232 parameters that are to be used for the data connection to that port (e.g. baud rate).

Then you must select what mode the port is to operate in. Each port can be set to support one of five operating modes:

I. Console Server mode enables remote network access to the attached devices serial console port

II. SDT mode enables graphical console (RDP, VNC, HTTPS etc) access to hosts that are serially connected

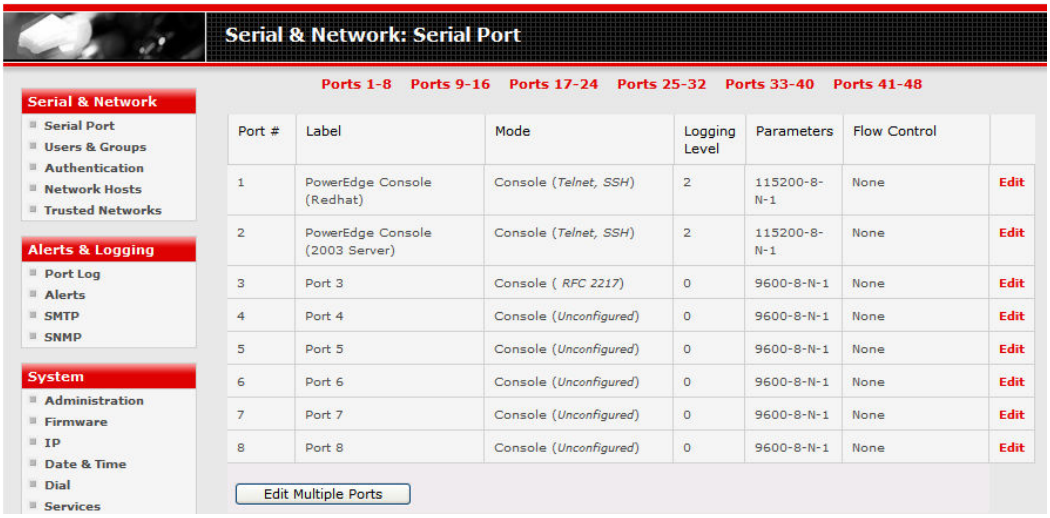
III. Power Device mode sets up the serial port to communicate with an intelligent serial controlled power strip (which are then controlled as detailed in *Chapter 8*)

IV. Terminal Server mode sets the serial port to await an incoming terminal login session

V. Serial Bridge mode enables the transparent interconnection of two serial port devices over a network

You can also configure the IMG/IM/CM4000 to support the remote syslog protocol on a per serial port basis.

Refer *Chapter 10 – Nagios Integration* for details on configuring the serial port to be monitored using the IMG/IM/CM4000 distributed Nagios monitoring

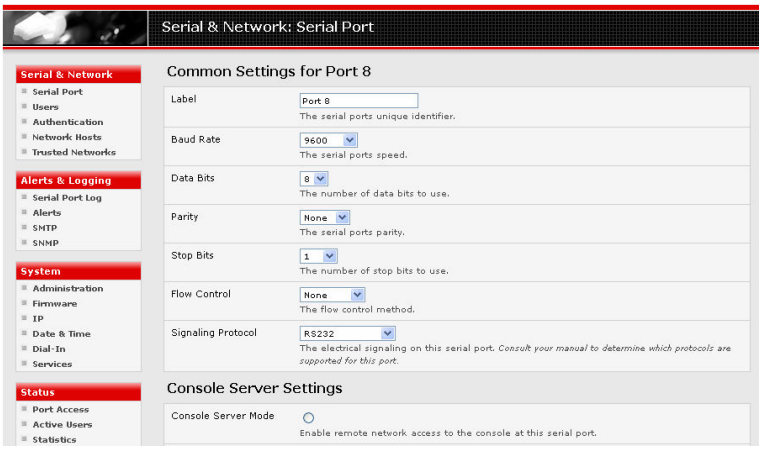


- Select **Serial & Network: Serial Port** and you will see the current labels, modes, and RS232 protocol options that are currently set up for each serial port
- By default each serial port is set in Console Server mode. For the port to be reconfigured click **Edit**
- When you have reconfigured the common settings (*Chapter 4.1.1*) and the mode (*Chapters 4.1.2 - 4.1.6*) for each port, you set up any remote syslog (*Chapter 4.1.7*), then click **Apply**

> **Note** If you wish to set the same protocol options for multiple serial ports at once:
>
> - Click **Edit Multiple Ports** and select which ports you wish to configure as a group

4.1.1 Common Settings

There are a number of common settings that can be set for each serial port. These are independent of the mode in which the port is being used. These serial port parameters must be set so they match the port parameters of the devices you attach to that port:



- Specify a label for the port
- Select the appropriate **Baud Rate**, **Parity**, **Data Bits**, **Stop Bits** and **Flow Control** for each port. (Note that the RS485 field is not relevant for IMG/IM/CM4000 gateways)

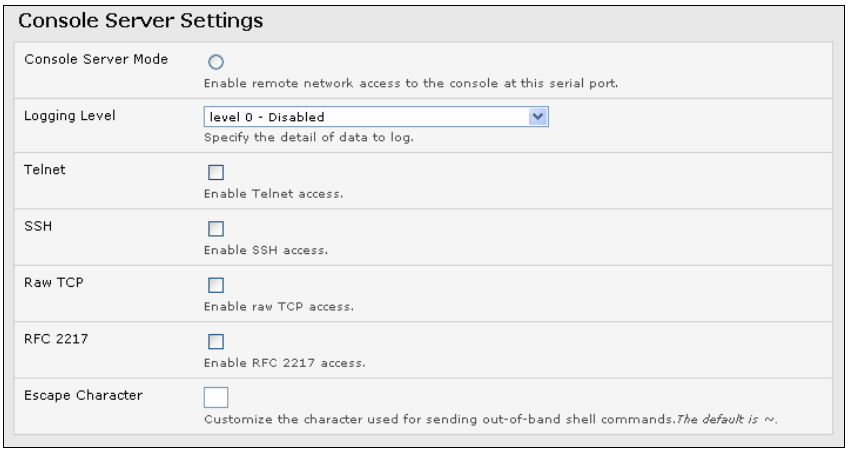
- Before proceeding with further serial port configuration, you should connect the ports to the serial devices they will be controlling, and ensure they have matching settings

Note The serial ports are all set at the factory to RS232 9600 baud, no parity, 8 data bits, 1 stop bit and Console Server Mode.

The baud rate can be changed to 2400 – 230400 baud using the management console. Lower baud rates (50, 75, 110, 134, 150, 200, 300, 600, 1200, 1800 baud) can be configured from the command line. Refer *Chapter 15 – Basic Configuration (Linux Commands)*

4.1.2 Console Server Mode

Select **Console Server Mode** to enable remote management access to the serial console that is attached to this serial port:



Logging Level specifies the level of information to be logged and monitored (refer *Chapter 7 - Alerts and Logging)*

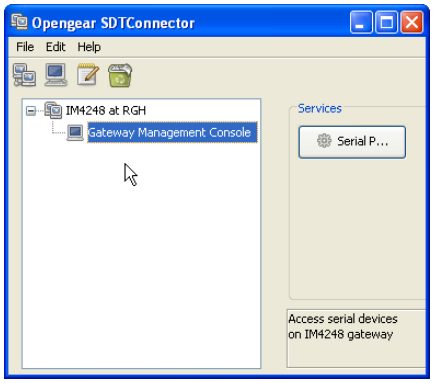
Telnet With the Telnet service enabled on the IMG/IM/CM4000, a Telnet client on a User or Administrator's PC/workstation can connect to a serial device attached

to this serial port on the gateway. The Telnet communications are unencrypted so this protocol is generally recommended only for local connections.

- From Win2000/XP/ NT, you can run *telnet* from the command prompt (*cmd.exe*)
- You can also use standard communications packages like *PuTTY* to set a direct Telnet (or SSH) connection to the serial ports (see box below)
- Also if the remote communications are being tunneled with *SDTConnector*, then Telnet can be used for securely accessing these attached devices (see box below).

Note In Console Server mode, Users and Administrators can use *SDTConnector* to set up secure Telnet connections that are SSH tunneled from their client PC/workstations to the serial port on the IM/CM4000. SDTConnector then enables those secure Telnet connections to be selected with a simple point-and-click.

To use *SDTConnector* to access consoles on the IM/CM4000 serial ports, you configure *SDTConnector* with the IM/CM4000 as a *gateway*, then as a *host*, and you enable Telnet service on Port (2000 + serial port #) *i.e.* 2001–2048. *Chapter 6- Secure Tunneling* has more information on using *SDTConnector* for Telnet and SSH access to devices that are attached to the IM/CM4000 gateway serial ports.

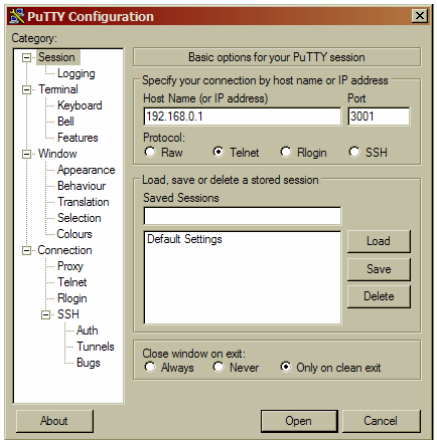


SDTConnector can be installed on Windows 2000, XP, 2003, Vista PCs and on most Linux platforms. Solaris platforms are also supported however they must have Firefox installed. For more general information on configuring and using *SDTConnector* refer to the **SDTConnector User Manual** on the IM/CM4000 CD (or online at ftp://ftp.opengear.com/manual/)

Note *PuTTY* also supports Telnet (and SSH) and the procedure to set up a Telnet session is simple.

Enter the IM/CM4000 gateway's IP address as the 'Host Name (or IP address)'. Select 'Telnet' as the protocol and set the 'TCP port' to 2000 plus the physical serial port number (*i.e.* 2001 to 2048).

Click the 'Open' button. You may then receive a 'Security Alert' that the host's key is not cached, you will need to choose 'yes' to continue. You will then be presented with the login prompt of the remote system connected to the serial port chosen on the IM/CM4000 device. You can login as normal and use the host serial console screen.



PuTTY can be downloaded at http://www.tucows.com/preview/195286.html

SSH It is recommended that you use SSH as the protocol where the User or Administrator connects to the IMG/IM/CM4000 gateway (or connects to the attached serial consoles) over the Internet or any other public network. This will provide authenticated SSH communications between the SSH client program on the remote user's PC/workstation and the gateway, so the user's communication with the serial device attached to the gateway is secure

For SSH access to the consoles on devices attached to the IMG/IM/CM4000 serial ports, you can use *SDTConnector*. You configure *SDTConnector* with the IMG/IM/CM4000 as a *gateway*, then as a *host*, and you enable SSH service on Port (3000 + serial port #) *i.e.* 3001-3048. *Chapter 6 - Secure Tunneling* has more information on using *SDTConnector* for SSH access to devices that are attached to the IMG/IM/CM4000 gateway serial ports.

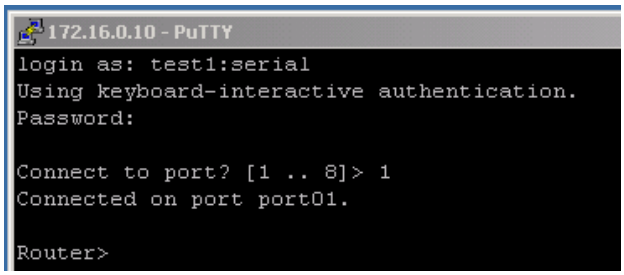
Also you can use common communications packages, like *PuTTY* or *SSHTerm* to SSH connect directly to port address IP Address _ Port (3000 + serial port #) *i.e.* 3001–3048

Alternately SSH connections can be configured using the standard SSH port 22. The serial port being accessed is then identified by appending a descriptor to the username. This syntax supports any of:

<username>:<portXX>
<username>:<port label>
<username>:<ttySX>
<username>:<serial>

So for a User named 'fred' to access serial port 2, when setting up the SSHTerm or the PuTTY SSH client, instead of typing *username = fred* and *ssh port = 3002*, the alternate is to type *username = fred:port02 (*or *username = fred:ttyS1)* and *ssh port = 22.*

Or, by typing *username=fred:serial* and *ssh port = 22,* the User is presented with a port selection option:



This syntax enables Users to set up SSH tunnels to all serial ports with only a single IP port 22 having to be opened in their firewall/gateway

TCP RAW TCP allows connections directly to a TCP socket. However while communications programs like *PuTTY* also supports RAW TCP, this protocol would usually be used by a custom application

For RAW TCP, the default port address is IP Address _ Port (4000 + serial port #) *i.e.* 4001 – 4048

RAW TCP also enables the serial port to be tunneled to a remote IMG/IM/CM4000 client gateway, so two serial port devices can be

transparently interconnect over a network (see *Chapter 4.1.6 – Serial Bridging*)

RFC2217 Selecting RFC2217 enables serial port redirection on that port. For RFC2217, the default port address is IP Address _ Port (5000 + serial port #) *i.e.* 5001 – 5048

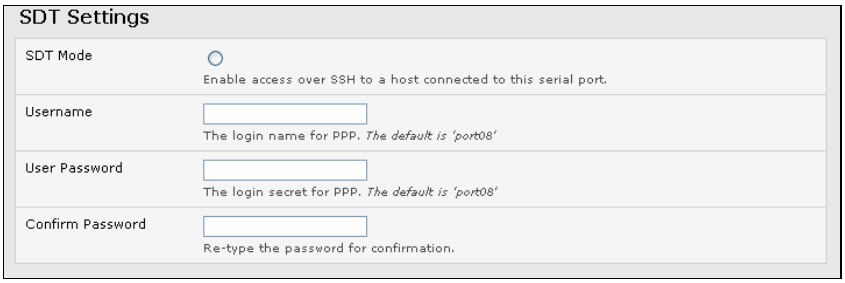
Special client software is available for Windows UNIX and Linux that supports RFC2217 virtual com ports, so a remote host can monitor and manage remote serially attached devices, as though they were connected to the local serial port. (see *Chapter 4.6 – Serial Port Redirection* for details)

RFC2217 also enables the serial port to be tunneled to a remote IMG/IM/CM4000 client gateway, so two serial port devices can be transparently interconnect over a network (see *Chapter 4.1.6 – Serial Bridging*)

Escape Character This enables you to change the character used for sending escape characters. The default is **~**.

4.1.3 SDT Mode

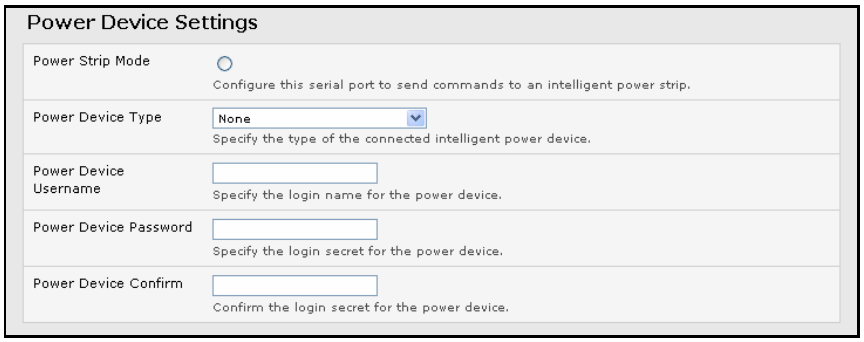
This Secure Tunneling setting allows port forwarding of RDP, VNC, HTPP, HTTPS, SSH, Telnet and other LAN protocols through to computers which are locally connected to the IMG/IM/CM4000 by their serial COM port. However such port forwarding requires a PPP link to be set up over this serial port.



Refer to *Chapter 6.6 - Using SDTConnector to Telnet or SSH connect to devices that are serially attached to the gateway* for configuration details

4.1.4 Power Strip Mode

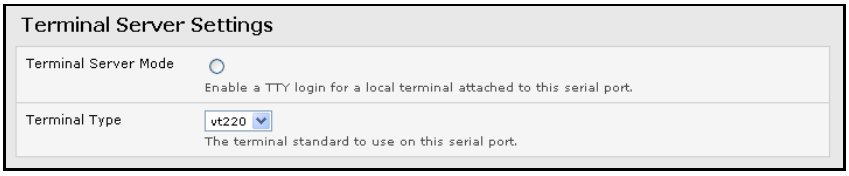
This mode configures the selected serial port to communicate with an intelligent serial controlled power strip:



Refer to *(Chapter 8.1 - Configuring Serial Port Power Strips)* for configuration details

4.1.5 Terminal Server Mode

- Select **Terminal Server Mode** and the **Terminal Type** (vt220, vt102, vt100, Linux or ANSI) to enable *agetty* on the selected serial port.



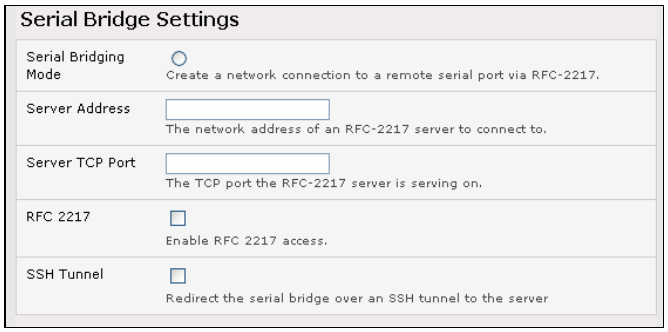
The *getty* will then configure the port and wait for a connection to be made. An active connection on a serial device is usually indicated by the Data Carrier Detect (DCD) pin on the serial device being raised. When a connection is detected, the *getty* program issues a login: prompt, and then invokes the login program to handle the actual system login.

Note Selecting Terminal Server mode will disable Port Manager for that serial port, so data is no longer logged for alerts etc.

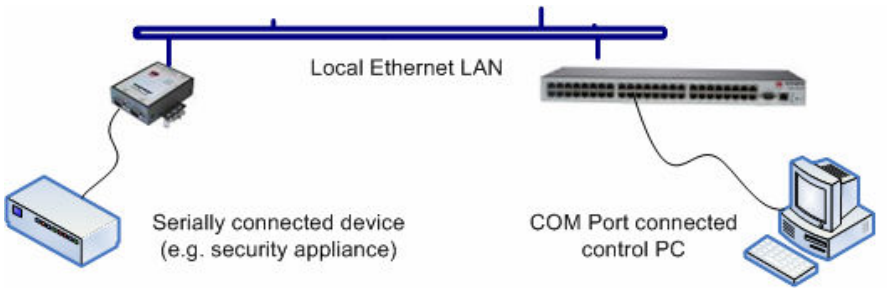
4.1.6 Serial Bridging Mode

Serial bridging is the encapsulation of serial data into network packets and the transport of the data over a network. So two IMG/IM/CM4000 gateways can configured to act as a virtual serial cable over IP network.

One gateway is configured as the server in Console Server mode with either RFC2217 or RAW enabled on the serial port to be bridged (as described in *Chapter 4.1.2 – Console Server Mode*). For the client gateway, the serial port must be set in Bridging Mode:



- Select **Serial Bridging Mode** and specify the IP address of the first IMG/IM/CM4000 gateway and the TCP port address of the remote serial port (for RFC2217 bridging this will be 5001-5048)
- By default the bridging client will use RAW TCP so you must select RFC2217 if this is the console server mode you have specified on the server gateway
- You may secure the communications over the local Ethernet by enabling SSH however you will need to generate and upload keys (refer *Chapter 14 – Advanced Configuration*)



4.1.7 Syslog

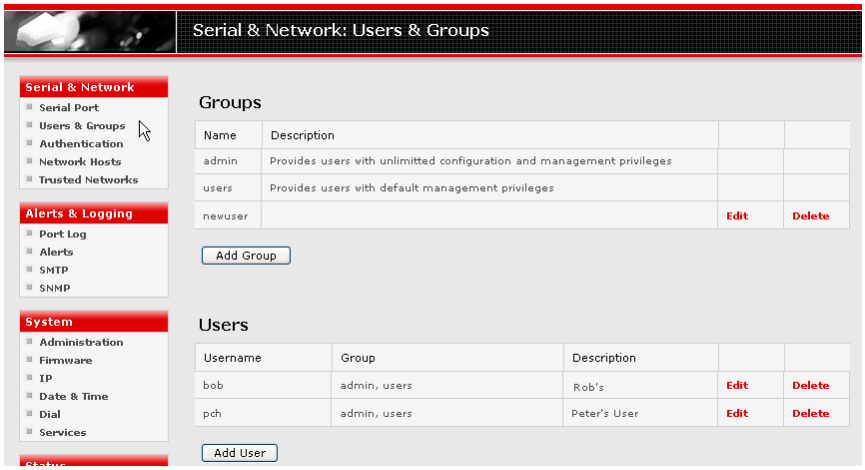
In addition to inbuilt logging and monitoring (which can be applied to serial-attached and network-attached management accesses, as covered in *Chapter 7 - Alerts and Logging*) the IMG/IM/CM4000 can also be configured to support the remote syslog protocol on a per serial port basis:

- Select the **Syslog Facility/Priority** fields to enable logging of traffic on the selected serial port to a syslog server; and to appropriately sort and action those logged messages (i.e. redirect them/ send alert email etc.)

For example if the computer attached to serial port 3 should never send anything out on its serial console port, the Administrator can set the **Facility** for that port to *local0* (*local0 .. local7* are meant for site local values), and the **Priority** to *critical*. At this priority, if the IMG/IM/CM4000 syslog server does receive a message, it will automatically raise an alert. Refer to *Chapter 7 - Alerts & Logging.*

4.2 Add / Edit Users

The Administrator uses this menu selection to set up, edit and delete Users and to define the access permissions for each of these Users.



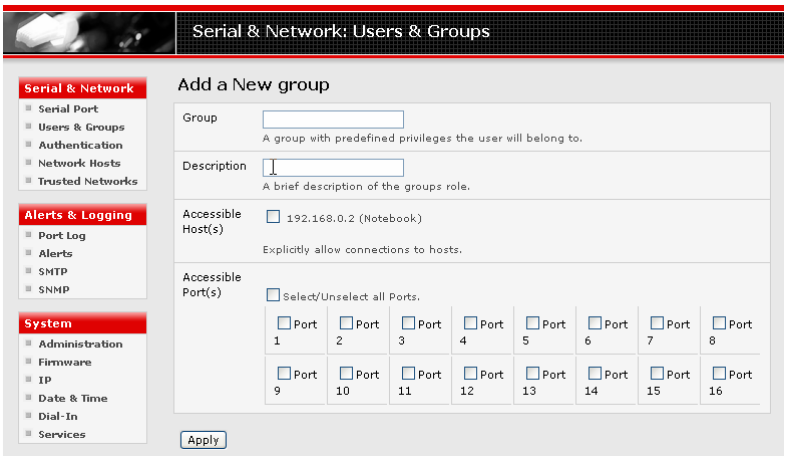
Users can be authorized to access specified IMG/IM/CM4000 serial ports and specified network-attached hosts. These Users can also be given full Administrator status (with full configuration and management and access privileges).

To simplify User set up, they can be configured as members of Groups. There are two Groups set up by default:

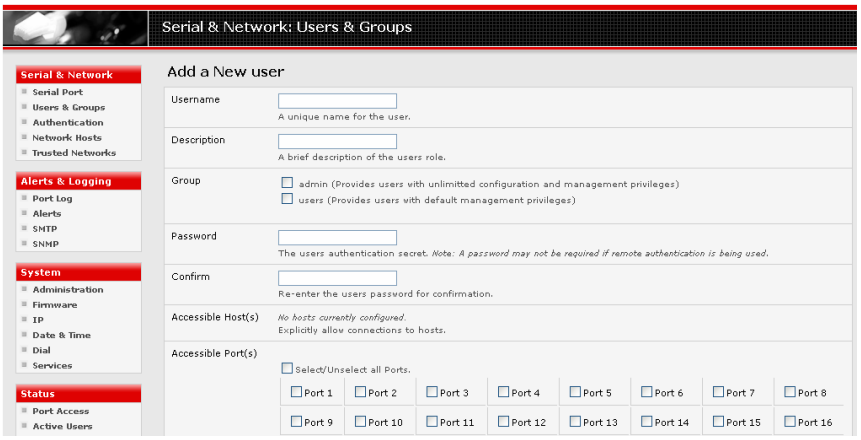
- **admin** which provides User members with full Administrator privileges
- **users** which provides User members with access to the Management section of the Management Console

The Administrator can also set up additional Groups with specific the serial ports and hosts access permissions. New Users can then be classified as members of particular Groups.

- Select **Serial & Network: Users & Groups** to display the configured Groups and Users
- Click **Add Group** to add a new Group



- Add a **Group** name and **Description** for each new Group, then nominate **Accessible Hosts** and **Accessible Ports** to specify the serial ports and hosts you wish any Users in this new Group to be able to access
- Click **Apply**
- Select **Serial & Network: Users** to display the configured Users
- Click **Add User** to add a new User



- Add a **Username** and a confirmed **Password** for each new User. You may also include information related to the User (*e.g.* contact details) in the **Description** field
- Nominate **Accessible Hosts** and **Accessible Ports** to specify which serial ports and which LAN connected hosts you wish the User to have access to

- Specify which **Group** (or Groups) you wish the User to be a member of.
- Click **Apply**

Your new User will now be able to access the nominated LAN devices and the devices attached to the nominated serial ports.

Note There are no limits on the number of Users you can set up; nor on the number of Users per serial port or host. So multiple Users (and the Administrator) can control /monitor the one port or host.

Each User can be a member of a number of Groups, in which case they take on the cumulative access privileges of each of those Groups. A User may not be a member of any Groups (however if the User is not even a member of the default *user* group will then they will not be able to use the IM/CM4000 Management Console to manage ports.

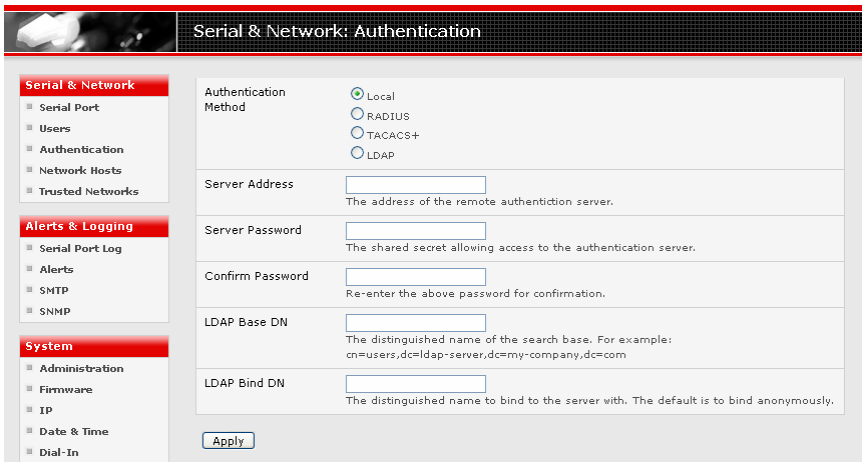
For more information on enabling the Secure Tunneling (RPD/ VNC/ Telnet/ HHTP/HTTPS/ SoL etc) access each User has to the network connected hosts refer *Chapter 6*.

The Administrator can also edit the access settings for any existing Users:

- Select **Serial & Network: Users & Groups** and click **Edit** for the User to be modified

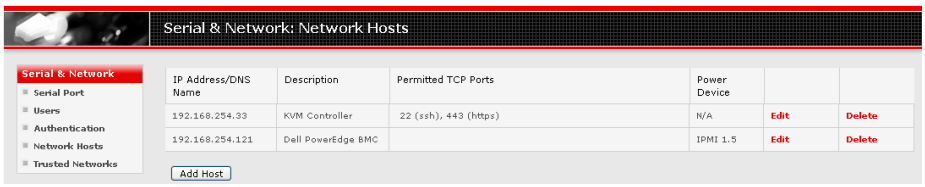
4.3 Authentication

Refer to *Chapter 9.1 - Remote Authentication Configuration* for authentication configuration details


Serial & Network: Authentication
Serial & Network
Serial Port
Users
Authentication
Network Hosts
Trusted Networks
Alerts & Logging
Serial Port Log
Alerts
SMTP
SNMP
System
Administration
Firmware
IP
Date & Time
Dial-In
Authentication Method
Local
RADIUS
TACACS+
LDAP
Server Address
The address of the remote authentiction server.
Server Password
The shared secret allowing access to the authentication server.
Confirm Password
Re-enter the above password for confirmation.
LDAP Base DN
The distinguished name of the search base. For example: cn=users,dc=ldap-server,dc=my-company,dc=com
LDAP Bind DN
The distinguished name to bind to the server with. The default is to bind anonymously.
Apply

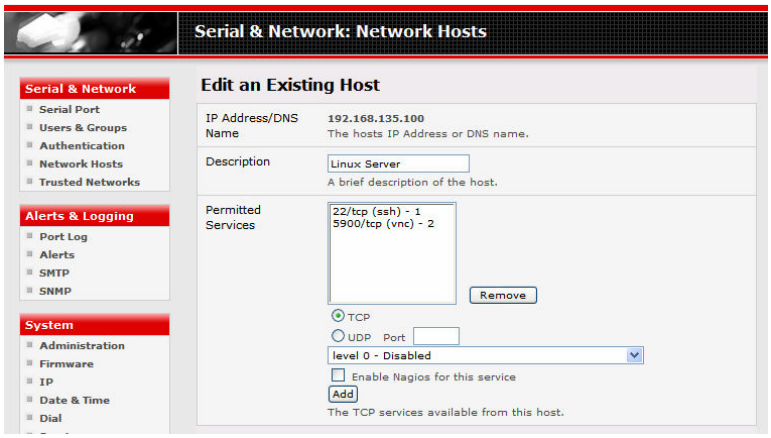
4.4 Network Hosts

To access a locally networked computer or appliance (referred to as a *Host*) you must identify the network connected Host; and then specify the TCP or UDP ports/services that will be used to control that Host



- Selecting **Serial & Network: Network Hosts** presents all the network connected Hosts that have been enabled for access, and the related access TCP ports/services

- Click **Add Host** to enable access to a new Host (or select **Edit** to update the settings for existing Host)



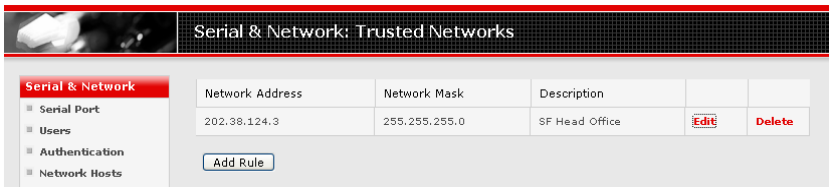
- Enter the **IP Address** or **DNS Name** of the new network connected Host (and optionally enter a **Description**)

- Add or edit the **Permitted Services** (or TCP/UDP port numbers) that are authorized to be used in controlling this host. Only these *permitted services* will be forwarded through by SDT to the Host. All other services (TCP/UDP ports) will be blocked.

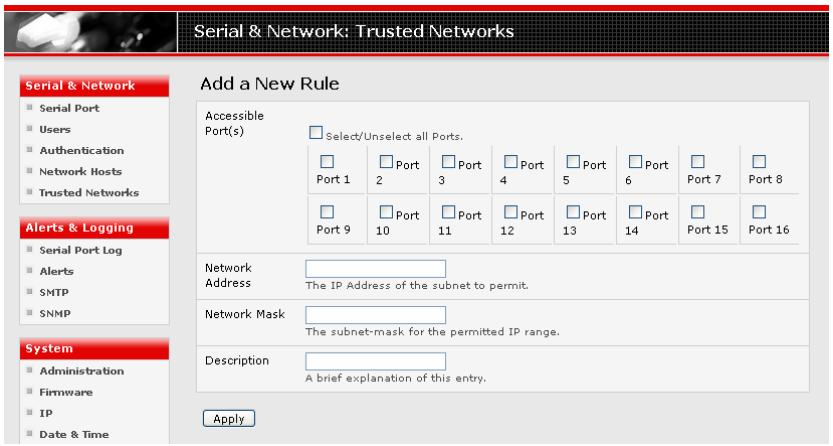
- Select **Nagios Enabled** if the service on the Host is to be monitored using the IMG/IM/CM4000 distributed Nagios monitoring For more details refer *Chapter 10 – Nagios Integration*
- The **Logging Level** specifies the level of information to be logged and monitored for each Host access (refer *Chapter 7 - Alerts and Logging*)
- If the Host is a networked server with IPMI power control, then the Administrator can enable users (Users and Administrators) to remotely cycle power and reboot. For more details refer *Chapter 8.2 - Configuring IPMI Power Management*
- Click **Apply**

4.5 Trusted Networks

The **Trusted Networks** facility gives you an option to nominate specific IP addresses that users (Administrators and Users) must be located at, to have access to the IMG/IM/CM4000 serial ports.



- Select **Serial & Network: Trusted Networks**
- To add a new trusted network, select **Add Rule**



- Select the **Accessible Port(s)** that the new rule is to be applied to
- Then enter the **Network Address** of the subnet to be permitted access
- Then specify the range of addresses that are to be permitted by entering a **Network Mask** for that permitted IP range *e.g.*
  - To permit all the users located with a particular Class C network (204.15.5.0 say) connection to the nominated port then you would add the following Trusted Network New Rule:

Network IP Address	204.15.5.0
Subnet Mask	255.255.255.0

  - If you want to permit only the one users who is located at a specific IP address (204.15.5.13 say) to connect:

Network IP Address	204.15.5.0
Subnet Mask	255.255.255.255

  - If however you want to allow all the users operating from within a specific range of IP addresses (say any of the thirty addresses from 204.15.5.129 to 204.15.5.158) to be permitted connection to the nominated port:

Host /Subnet Address	204.15.5.128
Subnet Mask	255.255.255.224

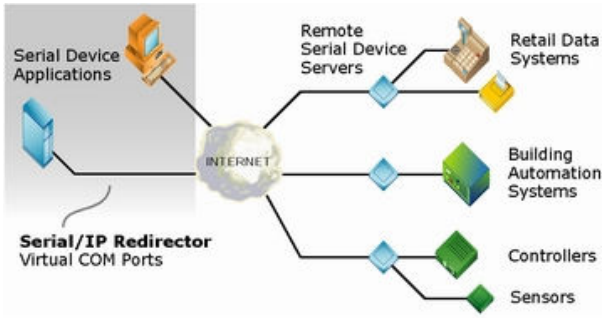
  - Click **Apply**

Note The above Trusted Networks will limit access by Users and the Administrator to the IM/CM4000 serial ports and network-attached hosts. However they do not restrict access by the Administrator to the IM/CM4000 console server itself. To change the default settings for this access, you will to need to edit the *IPtables* rules as described in the *Chapter 14 - Advanced.*

4.6 Serial Port Redirection Client

To access the virtual serial ports that RFC2217 support, you need to run client software (to actually redirect local serial ports to remote IMG/IM/CM4000 serial ports).

For Windows, Opengear recommends the Serial/IP™ COM Port Redirector from Tactical Software, which creates virtual COM ports for applications to use serial device servers without software changes. Tactical Software provides a trial copy of its products http://www.tacticalsoftware.com/products/serialip.htm



For Linux, AIX, HPUX, SCO, Solaris and UnixWare, Opengear has released an open source ***opengear-serial-client*** utility, which can be freely downloaded.

This serial port redirector software is loaded in your desktop PC, and it allows you to use a serial device connected to the remote IMG/IM/CM4000 as if it were connected to your local serial port. *opengear-serial-client* creates a pseudo tty port, connects the serial application to the pseudo tty port, receives data from the pseudo tty port, transmits it to the IMG/IM/CM4000 through network and receives data from the IMG/IM/CM4000 through network and transmits it to the pseudo-tty port.

Chapter 5 Failover and OoB Dial Access

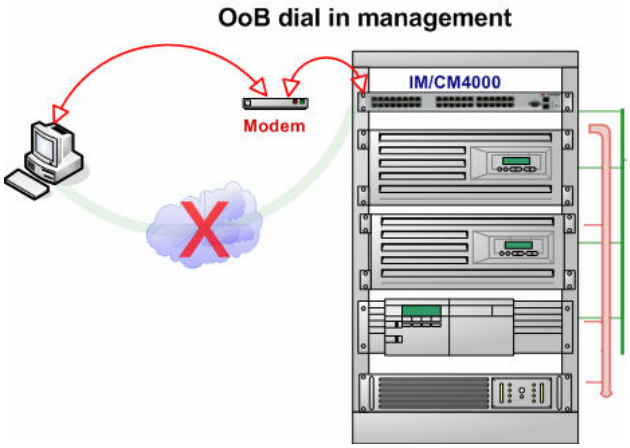
Introduction

The IMG/IM/CM4000 has a number of fail-over and out-of-band access capabilities to ensure high availability

- If there are difficulties in accessing the gateway through the principal network path, the Administrator can access the IMG/IM/CM4000 out-of-band (OoB) from a remote location using dial-up modem or ISDN connection
- The IM42xx and IMG4xxx can also be accessed out-of-band (OoB) using an alternate broadband link
- IM42xx and IMG4xxx gateways also offer broadband failover, so in the event of a disruption to the principal management network connection, access is switched transparently to the standby network connection
- The IM42xx and IMG4xxx can also be configured for out-dial failover, so in the event of a disruption in the principal management network, an external dial up ppp connection is established

5.1 OoB Dial-In access

To enable OoB dial-in access, you first configure the IMG/IM/CM4000 gateway (and once set up for dial-in PPP access, the gateway will await an incoming connection from a dial-in at remote site). Then set up the remote client dial-in software so it can establish a network connection from the Administrator's client modem to the dial in modem on the IMG/IM/CM4000.



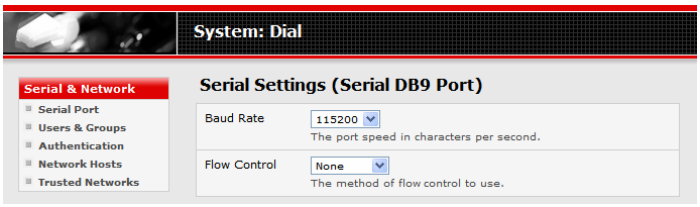
Note The IM42xx units are all supplied with an internal modem and a DB9 Local/Console port for OoB access. With the IM4200 units, an external modem can still be attached via a serial cable to the DB9 port, and the second Ethernet port can be configured for broadband OoB access.

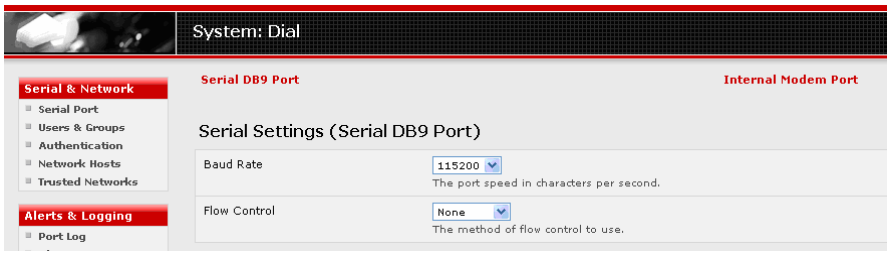
The IMG4216-25 has an internal modem as an option and supports broadband and external serial OoB access as above. The IMG4004-5 has the same OoB access facilities plus its supports PC card modems and wireless devices.

The CM4000 units need to have an external modem attached via a serial cable to their DB9 port. This port is marked *Local* and is located on the back of the CM4008/4001 unit, and the front of the CM4001/4116/4148 unit.

5.1.1 Configure Dial-In PPP

To enable dial-in PPP access on the IMG/IM/CM4000 console/modem port, or the IM42xx internal modem:





- Select the **System: Dial** menu option and the port to be configured (**Serial DB9 Port** or **Internal Modem Port**)

> **Note** The IMG/IM/CM4000 console/modem serial port is set by default to 115200 baud, No parity, 8 data bits and 1 stop bit, with software (Xon-Xoff) flow control enabled. When enabling OoB dial-in on CM4000 units it is recommended that this be changed to 38,4000 baud with Hardware Flow Control

- Select the **Baud Rate** and **Flow Control** that will communicate with the modem

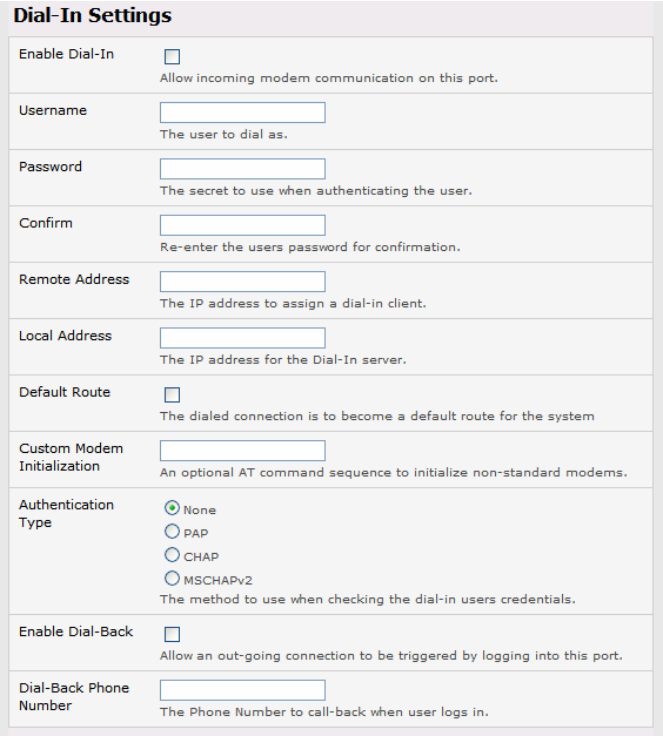
> **Note** You can further configure the console/modem port (*e.g.* to include *modem init* strings) by editing */etc/mgetty.config* files as described in the Chapter 14 - Advanced.

- Check the **Enable Dial-In Access** box
- Enter the **User name** and **Password** to be used for the dial-in PPP link
- In the **Remote Address** field, enter the IP address to be assigned to the dial-in client. You can select any address for the Remote IP Address. However it, and

the Local IP Address, must both be in the same network range (*e.g.* 200.100.1.12 and 200.100.1.67)

- In the **Local Address** field enter the IP address for the Dial-In PPP Server. This is the IP address that will be used by the remote client to access IMG/IM/CM4000 once the modem connection is established. Again you can select any address for the Local IP Address but it must both be in the same network range as the Remote IP Address

- The **Custom Modem Initialization** option allows a custom AT string modem initialization string to be entered (*e.g*. AT&C1&D3&K3)



- Then you must select the **Authentication Type** to be applied to the dial-in connection. The IMG/IM/CM4000 uses authentication to challenge Administrators who dial-in to the gateway. (For dial-in access, the username and password received from the dial-in client are verified against the local authentication database stored on the IMG/IM/CM4000). The Administrator must also have their client PC / workstation configured to use the selected authentication scheme. Select **PAP CHAP MSCHAPv2** or **None** and click **Apply**

None With this selection, no username or password authentication is required for dial-in access. This is not recommended.

PAP Password Authentication Protocol (PAP) is the usual method of user authentication used on the internet: sending a username and password to a server where they are compared with a table of authorized users. Whilst most common, PAP is the least secure of the authentication options.

CHAP Challenge-Handshake Authentication Protocol (CHAP) is used to verify a user's name and password for PPP Internet connections. It is more secure than PAP, the other main authentication protocol.

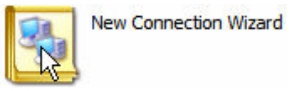
MSCHAPv2 Microsoft Challenge Handshake Authentication Protocol (MSCHAP) is authentication for PPP connections between a computer using a Microsoft Windows operating system and a network access server. It is more secure than PAP or CHAP, and is the only option that also supports data encryption

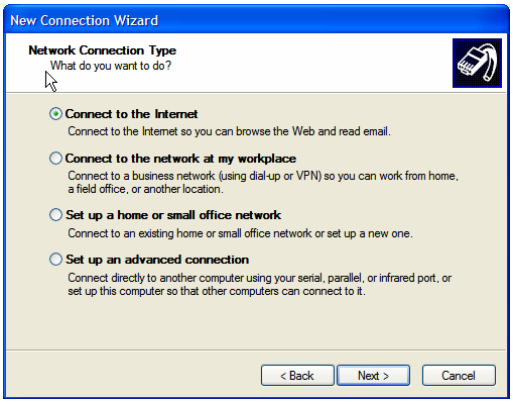
- IMG/IM/CM4000 gateways all support dial-back for additional security. Check the **Enable Dial-In Access** box and enter the phone number to be called to re-establish an OoB link once a dial-in connection has been logged

Note Chapter 13 (Advanced Configurations) has examples of Linux commands that can be used to control the modem port operation at the command line level

5.1.2 Set up Windows XP/ 2003 client

- Open **Network Connections** in Control Panel and click the **New Connection Wizard**





- Select **Connect to the Internet** and click **Next**
- On the **Getting Ready** screen select **Set up my connection manually** and click **Next**
- On the **Internet Connection** screen select **Connect using a dial-up modem** and click **Next**
- Enter a **Connection Name** (any name you choose) and the dial-up **Phone number** that will connect thru to the IMG/IM/CM4000 modem

- Enter the PPP **User name** and **Password** for have set up for the IMG/IM/CM4000

5.1.3 Set up earlier Windows clients

- For Windows 2000, the PPP client set up procedure is the same as above, except you get to the **Dial-Up Networking Folder** by clicking the **Start** button and selecting **Settings.** Then click **Network and Dial-up Connections** and click **Make New Connection**

- Similarly for Windows 98 you double click **My Computer** on the Desktop, then open **Dial-Up Networking** and double click **Make New Connection** and proceed as above

5.1.4 Set up Linux clients

The online tutorial http://www.yolinux.com/TUTORIALS/LinuxTutorialPPP.html presents a selection of methods for establishing a dial up PPP connection:

- Command line PPP and manual configuration (which works with any Linux distribution)
- Using the *Linuxconf* configuration tool (for Red Hat compatible distributions). This configures the scripts *ifup/ifdown* to start and stop a PPP connection
- Using the Gnome control panel configuration tool -
- WVDIAL and the Redhat "Dialup configuration tool"
- GUI dial program X-isp. Download/Installation/Configuration

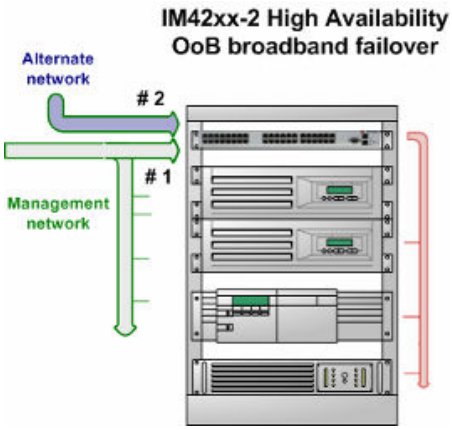
Note For all PPP clients:
- Set the PPP link up with TCP/IP as the only protocol enabled
- Specify that the Server will assign IP address and do DNS
- Do not set up the CM4000 PPP link as the default for Internet connection

5.1.5 Using SDTConnector client

Administrators can use their *SDTConnector* client to set up secure OoB dial-in access to remote IMG/IM/CM4000 gateways. The *SDTConnector* Java client software provides point-and-click secure remote access. For more information refer to the SDTConnector User Manual included on the IMG/IM/CM4000 CD.

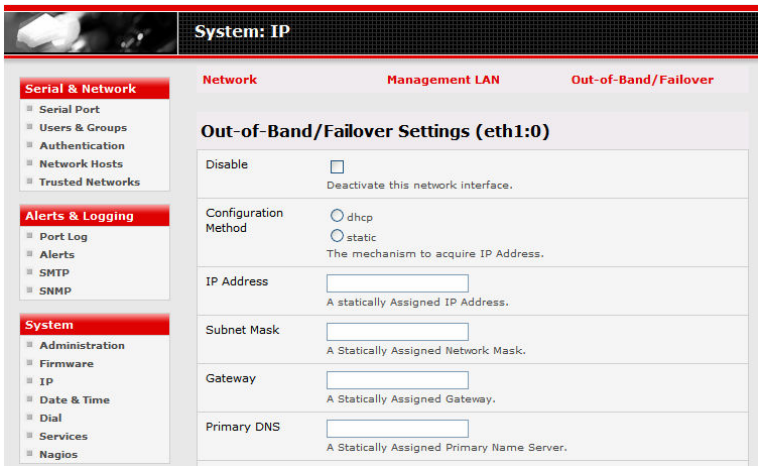
5.2 OoB broadband access (IMG4xxx and IM42xx only)

IMG/IM gateways have a second Ethernet port (*Network 2* on the IM42xx; Management LAN port 4 on the IMG4004-5; or Management LAN port 24 on the IMG4216-25) that can be configured for alternate and OoB (out-of-band) broadband access. With two active broadband access paths to the IM/IMG gateway, in the event you are unable to access through the primary management network (*Network or Network1*) you can still access it through the alternate broadband path (e.g. a T1 link):



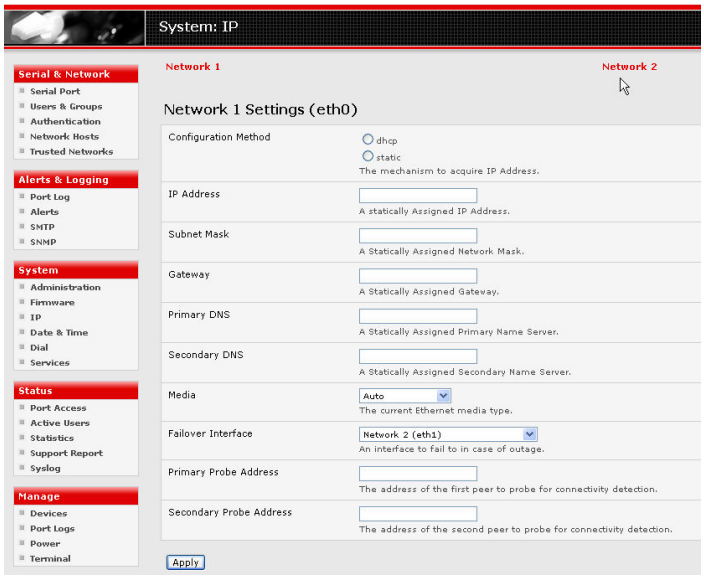
- On the **System: IP** menu select **Network 2** (IM42xx) or **Out of Band/ Failover** (IMG4xxx) and configure the **IP Address, Subnet Mask**, **Gateway** and **DNS** with the access settings that relate to the alternate link

- Ensure when configuring the principal **Network 1 Settings (eth0)** connection, the **Failover Interface** is set to *None*.

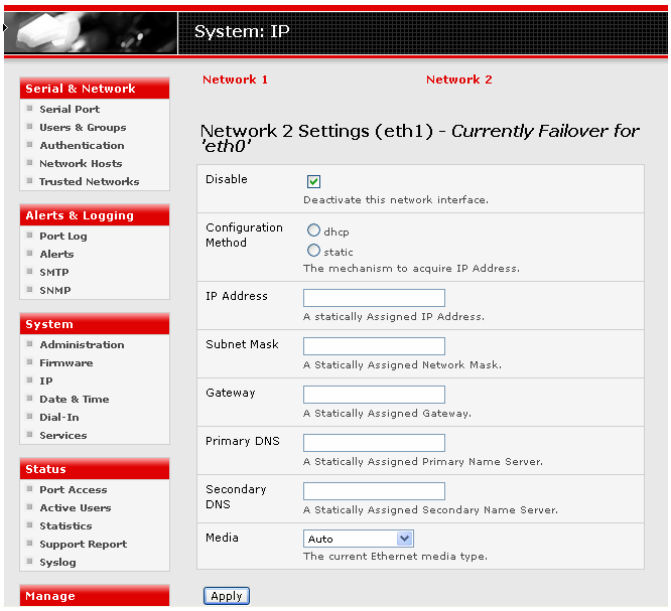


5.3 Broadband Ethernet Failover (IMG4xxx and IM42xx only)

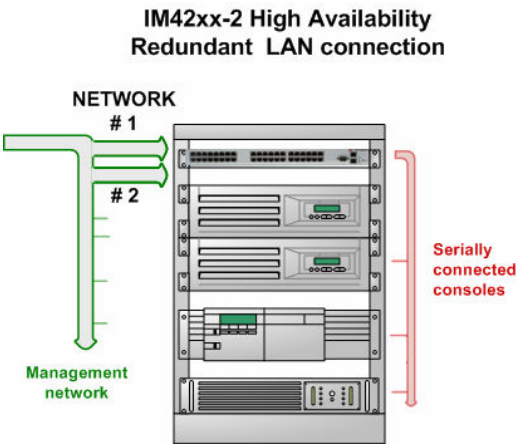
The second IM42XX Ethernet can also be configured for failover to ensure transparent high availability.



- When configuring the principal network connection, specify **Network 2 (eth1)** as the **Failover Interface** to be used when a fault has been detected with Network 1 (eth0)
- Specify the **Probe Addresses** of two sites (the **Primary** and **Secondary**) that the IMG/IM/CM4000 is to *ping* to determine if Network 1 (eth0) is still operational



- Then configure **Network 2 Settings (eth1)** with the same IP setting that you used for Network 1 (eth0) to ensure transparent redundancy



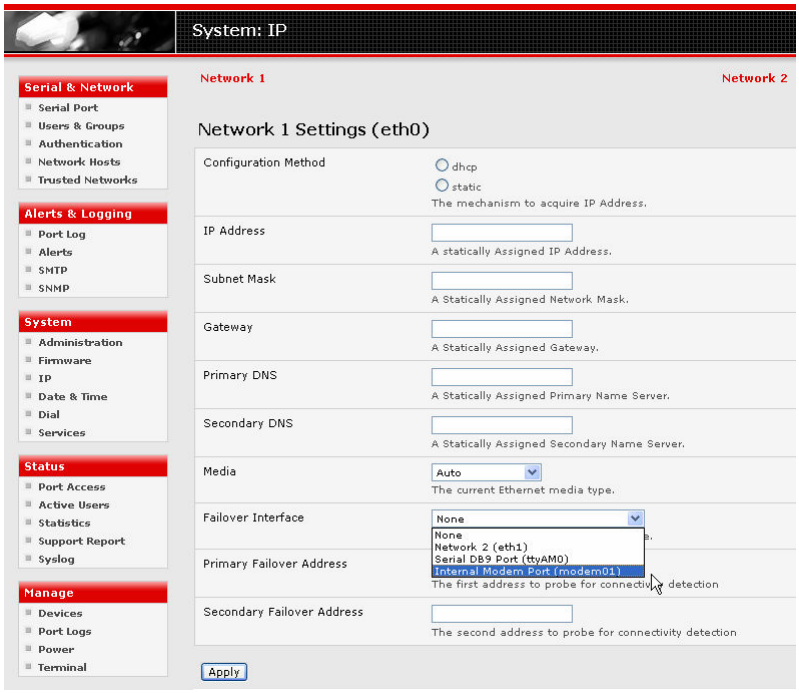
In this mode, Network 2 (eth1) is available as the transparent back-up port to Network 1 (eth0) for accessing the management network. Network 2 will automatically and transparently take over the work of Network 1, in the event Network 1 becomes unavailable for any reason. And when Network 1 becomes available again, it takes over the work again.

5.4 Dial-Out Failover (IMG4xxx and IM42xx only)

IMG/IM gateways can be configured so a dial-out PPP connection is automatically set up in the event of a disruption in the principal management network:

- When configuring the principal network connection in **System: IP**, specify **Internal Modem** (or the **Dial Serial DB9** if you are using an external modem on the Console port) as the **Failover Interface** to be used when a fault has been detected with Network / Network1 (eth0)

- Specify the **Probe Addresses** of two sites (the **Primary** and **Secondary**) that the IMG/IM gateway is to *ping* to determine if Network / Network1 is still operational

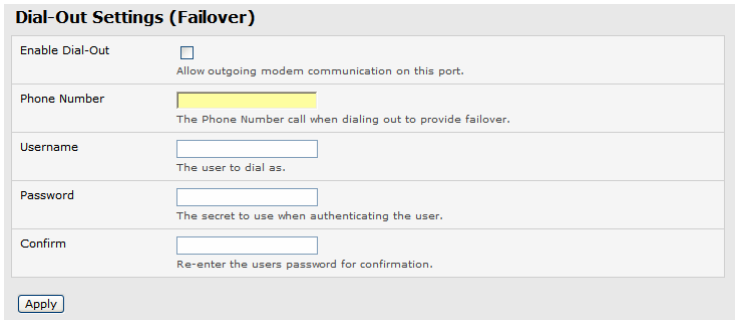


- Select the **System: Dial** menu option and the port to be configured (**Serial DB9 Port** or **Internal Modem Port**)

- Select the **Baud Rate** and **Flow Control** that will communicate with the modem

Note You can further configure the console/modem port (*e.g.* to include *modem init* strings) by editing */etc/mgetty.config* files as described in the Chapter 13 - Advanced.

- Check the **Enable Dial-Out Access** box and enter the access details for the remote PPP server to be called

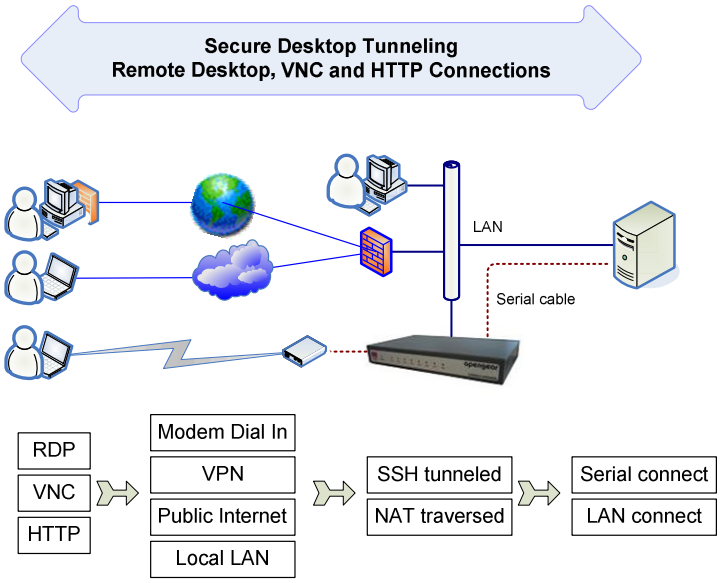


Chapter 6 Secure Tunneling

Introduction

Each Opengear gateway has an SDT Tunneling server embedded, so the one gateway can be used to securely manage all the systems and network devices in the data center - using text-based console tools (such as serial port SSH/telnet, SoL) or graphical desktop tools (VNC, RDP, HTTPS, HTTP, X11, DRAC, iLO etc).

SDT allows both end Users and Administrators to securely access and take remote control of any computer (Windows, Linux, UNIX, Solaris, Macintosh) using VNC or Microsoft's Remote Desktop protocol. SDT also provides browser and Telnet access, which enables secure remote control of network attached devices with browser or text control interfaces. SDT can also be configured to support any other TCP or UDP connection protocol (e.g. IPMI SoL or X11)



To set up Secure Tunnel access, the computer being accessed can be:

- located on the same local network as the IMG/IM/CM4000, or
- attached to the IMG/IM/CM4000 via its serial COM port.

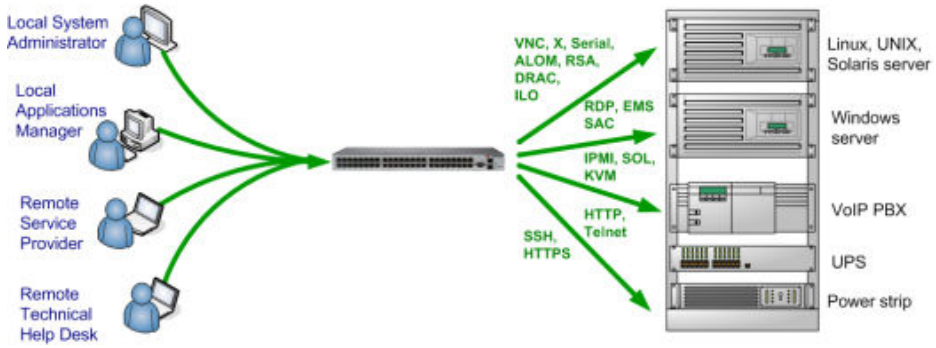
The remote User/Administrator then connects to the IMG/IM/CM4000 via:

- a secure dial-up or ISDN modem (thru an SSH tunnel)
- a secure broadband Internet connection (thru an SSH tunnel)
- the enterprise VPN network (preferably thru an SSH tunnel), or
- the local network (preferably thru an SSH tunnel)

This chapter details:

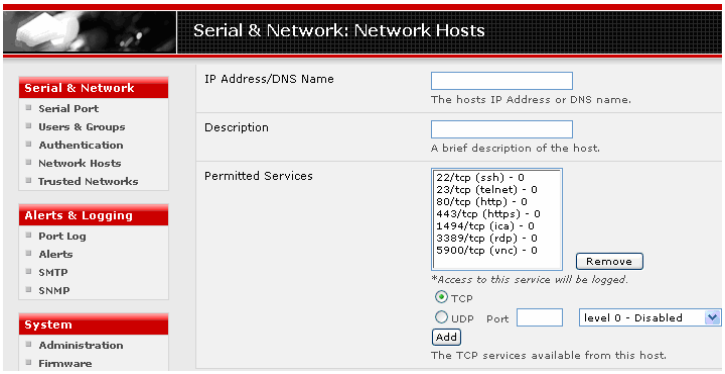
- Configuring the IMG/IM/CM4000 gateway for SDT access to network attached hosts and setting up permitted Services and Users access (*Section 6.1*)
- Set up the SDT connection between the Client PC and the gateway (*Section 6.2*)
- Setting up a SDT Secure Tunnel for Remote Desktop (*Section 6.3*)
- Setting up a SDT Secure Tunnel for VNC (*Section 6.4*)
- Using SDTConnector to browser access the gateway Management Console (*Section 6.5*)
- Using SDTConnector to Telnet or SSH connect to devices that are serially attached to the gateway(*Section 6.6*)
- Using SDT to IP connect to hosts that are serially attached to the gateway (*Section 6.7*)

6.1 Configuring for SDT Tunneling to hosts



To set up the IMG/IM/CM4000 gateway to SDT access a network attached *host*, the *host* and the permitted *services* that are to be used in accessing that host need to be configured on the gateway, and User access privileges need to specified:

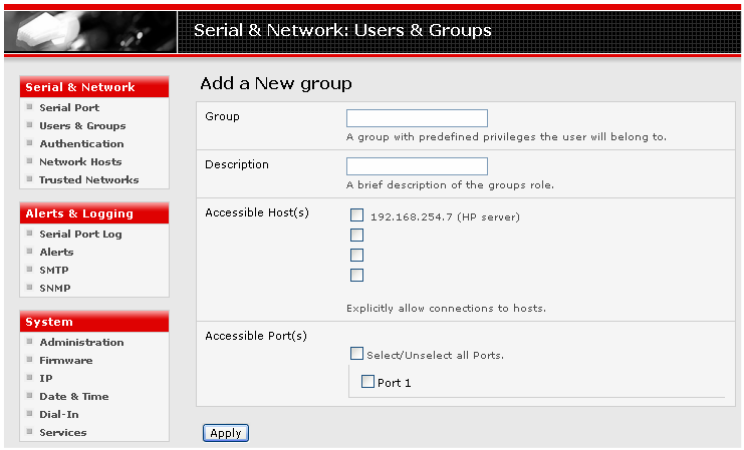
- Add the new *host* and the *permitted services* using the **Serial & Network: Network Hosts** menu as detailed in *Network Hosts (Chapter 4.4).* Only these *permitted services* will be forwarded through by SDT to the *host*. All other services (TCP/UDP ports) will be blocked.



Note Following are some of the TCP Ports used by SDT in the IMG/IM/CM4000:

22	SSH (All SDT Tunneled connections)
23	Telnet on local LAN (forwarded inside tunnel)
80	HTTP on local LAN (forwarded inside tunnel)
3389	RDP on local LAN (forwarded inside tunnel)
5900	VNC on local LAN (forwarded inside tunnel)
73XX	RDP over serial from local LAN – where XX is the serial port number (i.e. 7301to 7348 on CM4148)
79XX	VNC over serial from local LAN – where XX is the serial port number

- Add the new *Users* using **Serial & Network: Users & Groups** menu as detailed in *Network Hosts (Chapter 4.4)*. Users can be authorized to access the IMG/IM/CM4000 ports and specified network-attached hosts. To simplify configuration, the Administrator can first set up *Groups* with group access permissions, then Users can be classified as members of particular *Groups*.



6.2 Establish SSH connection between Client PC and gateway

6.2.1 Determine the gateway IP address

If the client PC is connecting to the IMG/IM/CM4000 through the public Internet, before you can set up the secure SSH tunnel, you will need to:

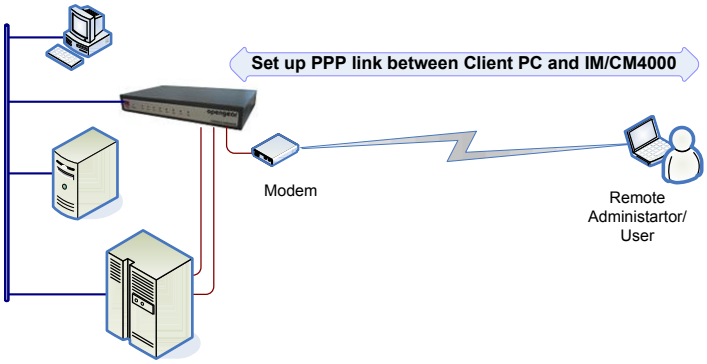
- Determine *the public IP address* of the IMG/IM/CM4000 (or of the router/firewall that connects the IMG/IM/CM4000 to the Internet) as assigned by the ISP. To find the public IP address, access from http://checkip.dyndns.org/ or http://www.whatismyip.com/ from a PC on the same network as the IMG/IM/CM4000 and note the reported IP address.

- Set port forwarding for TCP port 22 through any firewall/NAT/router that is located between the remote Client PC and the IMG/IM/CM4000 e.g. the following shows the SDT SSH port being forwarded on a Cisco/Links WAG54G DSL gateway so it points to port 22 on the IMG/IM/CM4000 that is located at 192.168.1.33

Note http://www.portforward.com has port forwarding instructions for a range of routers. Also you can use the Open Port Check tool from http://www.canyouseeme.org to check if port forwarding through local firewall/NAT/router devices has been properly configured

6.2.2 Dial in configuration

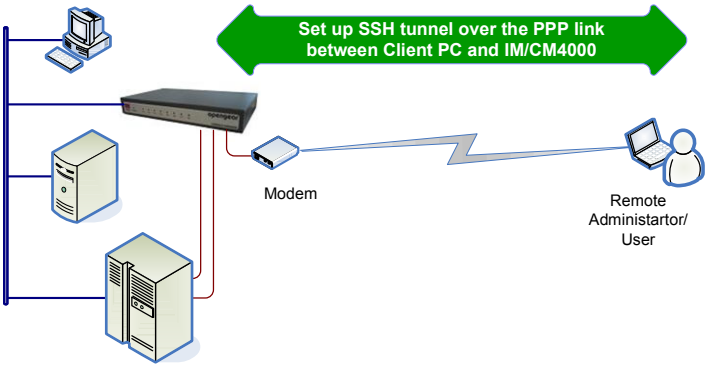
If the client PC is dialing into *Local/Console* port on the IMG/IM/CM4000 you will need to set up a dial-in PPP link:



- Configure the IMG/IM/CM4000 for dial-in access (following the steps in the ***Configuring for Dial-In PPP Access*** section in *Chapter 5*, *Configuring Dial In Access*)

- Set up the PPP client software at the remote User PC (following the ***Set up the remote Client*** section in *Chapter 5*)

Once you have a dial-in PPP connection established, you then can set up the secure SSH tunnel from the remote Client PC to the IMG/IM/CM4000.



6.2.3 Choosing an SSH client

To set up the secure SSH tunnel from the Client PC to the IMG/IM/CM4000, you must install and launch SSH client software on the Client PC. Opengear supplies and recommends you use the *SDTConnector* client software that is supplied with the gateway. *SDTConnector* is a Java client program that is couples the trusted SSH tunneling protocol with popular access tools such as Telnet, HTTP, HTTPS, VNC, RDP to provide point-and-click secure remote access to systems and devices inside your network.

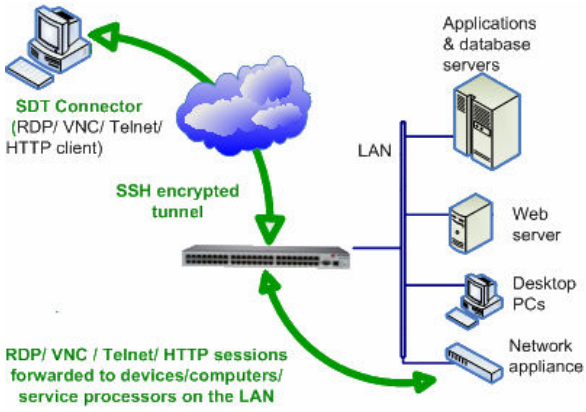
However there's also a wide selection of commercial and free SSH client programs that are supported:

- PuTTY is a complete (though not very user friendly:) freeware implementation of SSH for Win32 and UNIX platforms
- SSHTerm is a useful open source SSH communications package
- SSH Tectia is leading end-to-end commercial communications security solution for the enterprise
- Reflection for Secure IT (formerly F-Secure SSH) is another good commercial SSH-based security solution

6.2.4 Create the SSH tunnel using SDTConnector client

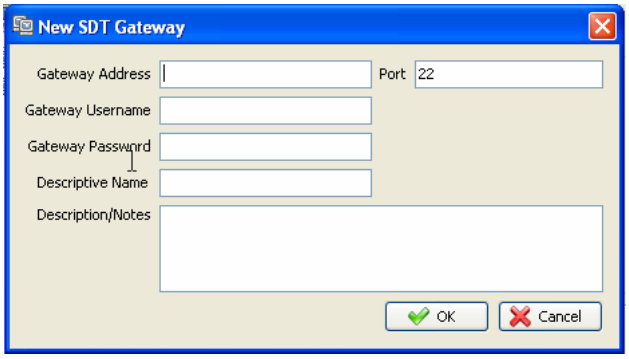
SDTConnector is a light weight tool that enables Users or Administrators to securely access and control host computers, networks and appliances at local and remote locations. *SDTConnector* does this by:

- setting up a secure SSH tunnel from the client PC to the selected IMG/IM/CM4000 gateway, then
- establishing a port forward connection from port 22 on the gateway to the nominated TCP/IP port connecting to the target host, then
- executing the appropriate client application that will be used in communicating with the host

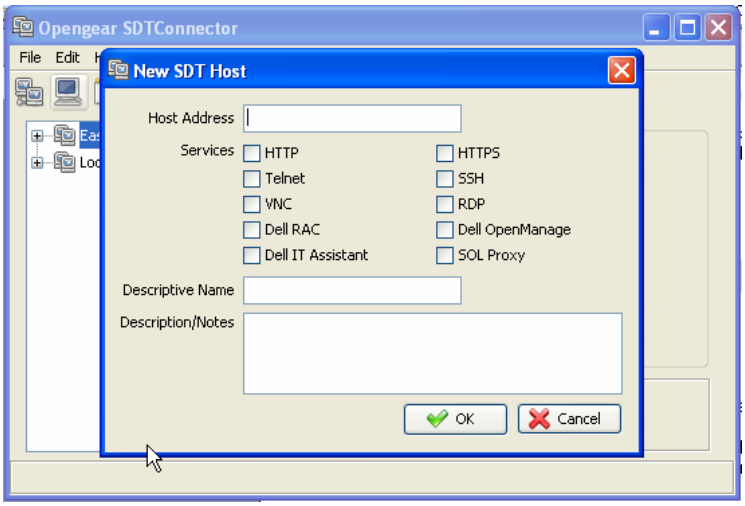


To operate *SDTConnector,* you will need to configure the client software by identifying the network connected hosts that can be accessed through the gateway,

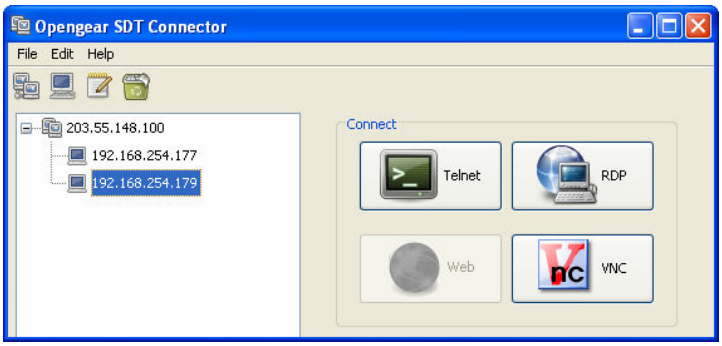
- Launch *SDTConnector* on your PC and select **File -> New Gateway** to add the IMG/IM/CM4000 as a *gateway* in your SDTConnector client (with username/ password etc)



- Select this newly added Gateway and click the Host icon to add new *hosts*. (Alternatively, select **File -> New Host**). Enter the Host IP Address and give some details in Descriptive Name/Notes.
- For each new host, specify the services (and the related IP ports) being redirected and client applications to be executed for each of these services. SDTConnector is preconfigured with a range of services and clients preconfigured (e.g. VNC, RDP, HTTP, HTTPS, IPMI1.5/2.0, SSH , Telnet, Dell RAC/ OpenManage/ SOLProxy)



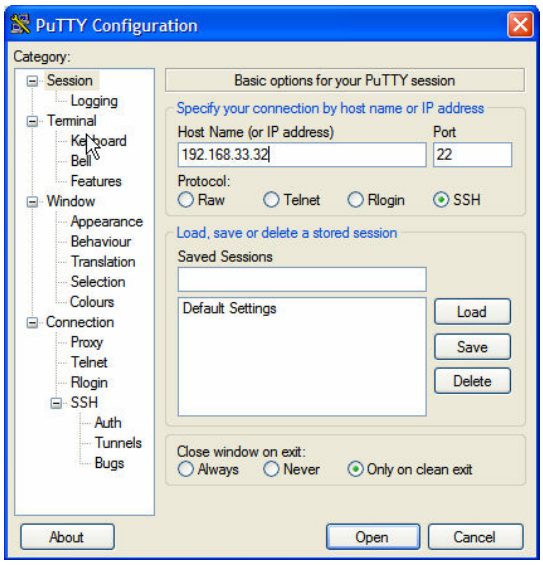
At this stage with a simple point-and-click *SDTConnector* will connect to the selected network connected host. You can also extend *SDTConnector* to add (or edit) services and related ports; and add (or edit) client applications that will executed when communicating with this host.



SDTConnector can be installed on Windows 2000, XP, 2003, Vista PCs and on most Linux, UNIX and Solaris. Full details on installing, configuring and using *SDTConnector* can be found in the **SDTConnector User Manual** (on the IMG/IM/CM4000 CD or online at *ftp://ftp.opengear.com/manual/*)

6.2.5 Create the SSH tunnel using PuTTY client

The steps below show the establishment of an SSH connection and then forwarding the RDP port over this SSH connection - using the PuTTY client software:



- Under the Session tab, enter the IP address of the IMG/IM/CM4000 in the **Host Name or IP address** field.

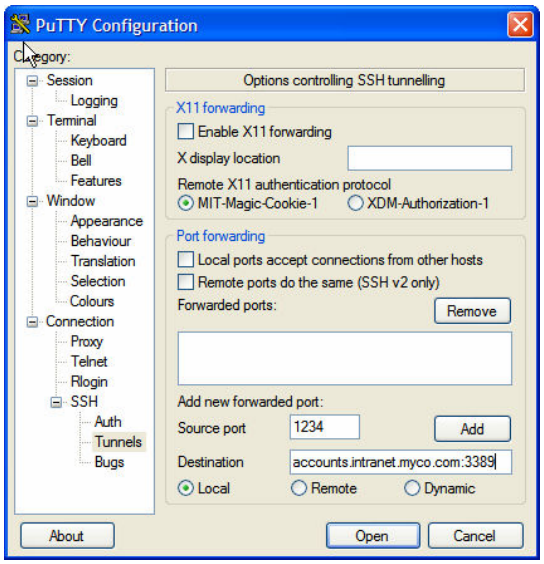
- For dial-in connections, this IP address will be the **Local** Address that you assigned to the IMG/IM/CM4000 when you set it up as the Dial-In PPP Server
- For Internet (or local/VPN connections) connections this will be the public IP address of the IMG/IM/CM4000

➢ Select the **SSH Protocol**, and the **Port** will be set as 22

➢ Under the **SSH -> Tunnels** tab, **Add new forwarded port** specifying the **Source port** as *1234* (or any number you choose)

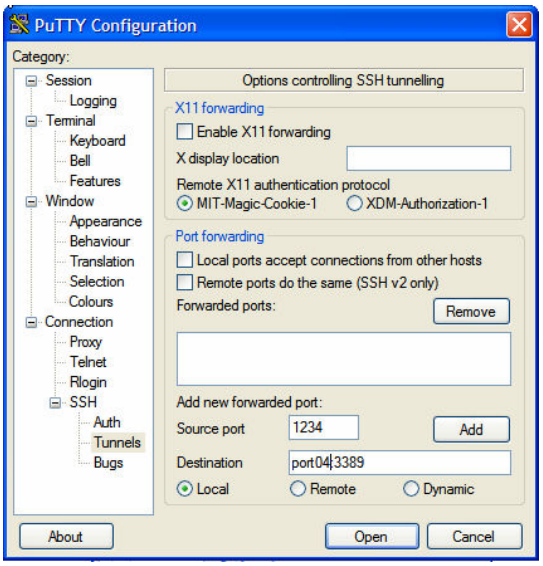
➢ Set the **Destination:**

- If your destination computer is network connected to the IMG/IM/CM4000, set the Destination as <*SDT Host IP address/DNS Name*>*:3389* e.g. if the SDT Host IP Address you specified when setting up the *SDT Hosts* on the IMG/IM/CM4000 was *accounts.myco.intranet.com*, then specify the Destination as *accounts.myco.intranet.com:3389*



- If your destination computer is serially connected to the IMG/IM/CM4000, set the *Destination* as <*port label*>*:3389* e.g. if the **Label** you specified on the SDT enabled serial port on the IMG/IM/CM4000 is *win2k3*, then specify the remote host as *win2k3:3389* . Alternative you can set the *Destination* as *portXX:3389* where XX is the SDT enabled serial port number e.g. if port 4 is on the IMG/IM/CM4000 is to carry the RDP traffic then specify *port04:3389*

Note http://www.jfitz.com/tips/putty_config.html has useful examples on configuring PuTTY for SSH tunneling

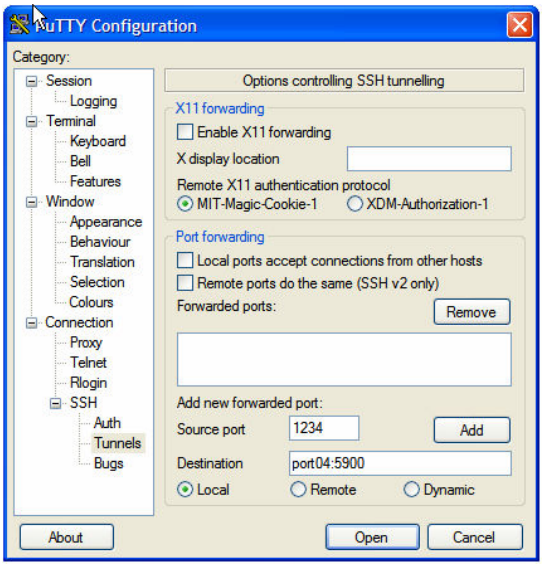


- Select **Local** and click the **Add** button
- Click **Open** to SSH connect the Client PC to the IMG/IM/CM4000
- You will now be prompted for the Username/Password for the IMG/IM/CM4000 User you SDT enabled

Note You can also secure the SDT communications from local and enterprise VPN connected Client PCs using SSH as above.

This will protect against the risk of the “man in the middle” attacks to which RDP has a vulnerability http://www.securiteam.com/windowsntfocus/5EP010KG0G.html

To set up the secure SSH tunnel from the Client (Viewer) PC to the IMG/IM/CM4000 for VNC follow the steps above, however when configuring the VNC port redirection specify port 5900 (rather than port 3389 as was used for RDP) e.g. if using PuTTY:



Note How secure is VNC?

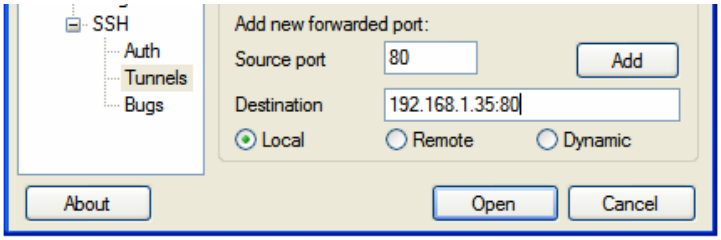
VNC access generally allows access to your whole computer, so security is very important. VNC uses a random challenge-response system to provide the basic authentication that allows you to connect to a VNC server. This is reasonably secure and the password is not sent over the network.

However, once connected, all subsequent VNC traffic is unencrypted. So a malicious user could snoop your VNC session. Also there are VNC scanning programs available, which will scan a subnet looking for PCs which are listening on one of the ports which VNC uses.

Tunneling VNC over a SSH connection ensures all traffic is strongly encrypted. Also no VNC port is ever open to the internet, so anyone scanning for open VNC ports will not be able to find your computers. When tunneling VNC over a SSH connection, the only port which you're opening on your IMG/IM/CM4000 the SDT port 22.

So sometimes it may be prudent to tunnel VNC through SSH even when the Viewer PC and the IMG/IM/CM4000 are both on the same local network.

To set up the secure SSH tunnel for a HTTP browser connection from the client PC, follow the steps above. However when configuring the port redirection, specify port 80 (rather than port 3389 as was used for RDP) e.g. if using PuTTY:

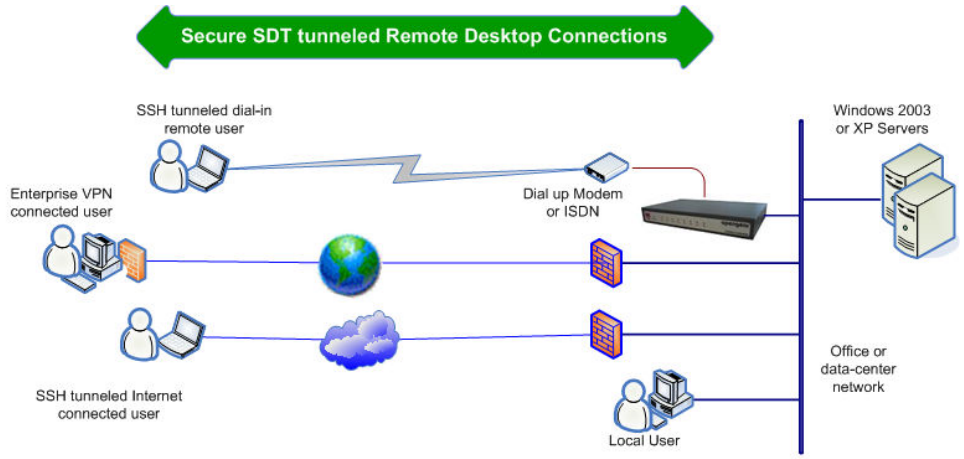


6.3 Setting up SDT for Remote Desktop access

Microsoft's Remote Desktop Protocol (RDP) enables the system manager to securely access and manage remote Windows computers – to reconfigure applications and user profiles, upgrade the server's operating system, reboot the machine etc. Opengear's Secure Tunneling uses SSH tunneling, so this RDP traffic is securely transferred through an authenticated and encrypted tunnel.

SDT with RDP also allows remote Users to connect to Windows XP, Windows 2003 computers and to Windows 2000 Terminal Servers; and to have access to all of the applications, files, and network resources (with full graphical interface just as though they were in front of the computer screen at work).

To set up a secure Remote Desktop connection you must enable Remote Desktop on the target Windows computer that is to be accessed and configure the RPD client software on the client PC.

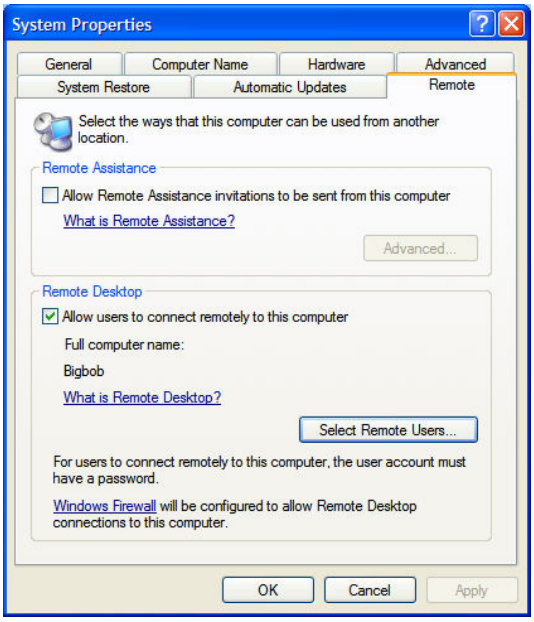


Secure RDP Tunnels

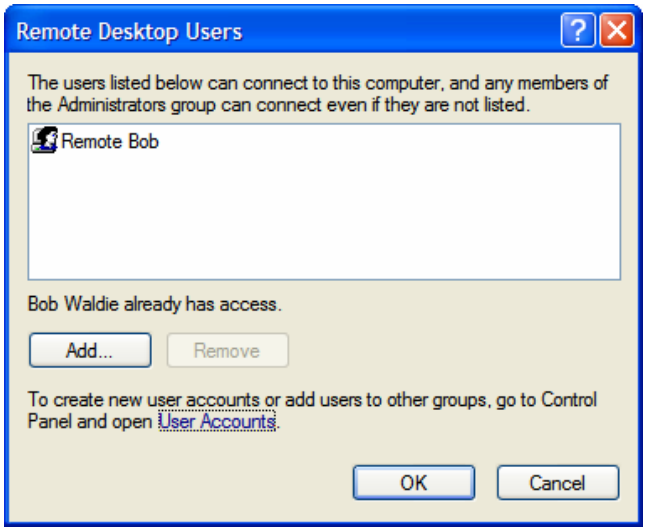
6.3.1 Enable Remote Desktop on the target Windows computer to be accessed

With Microsoft's Remote Desktop you can access and manage Windows XP Professional and Windows Server 2003 computers. To enable **Remote Desktop** on the Windows computer being accessed:

- Open **System** in the Control Panel and click the **Remote** tab



- Check **Allow users to connect remotely to this computer**
- Click **Select Remote Users**



- To set the user(s) who can remotely access the system with RDP click **Add** on the **Remote Desktop Users** dialog box

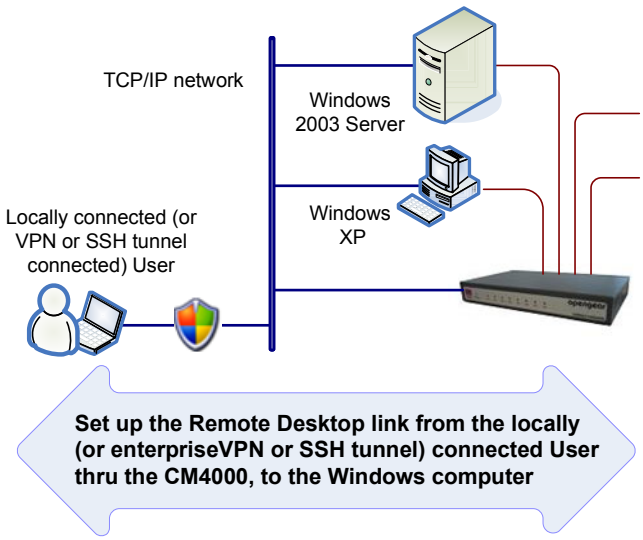
> **Note** If you need to set up new users for Remote Desktop access, open **User Accounts** in the Control Panel and proceed through the steps to nominate the new user's name, password and account type (Administrator or Limited)

Note With Windows XP Professional, you have only one Remote Desktop session and it connects directly to the Windows root console. With Windows Server 2003, you have the console session and two other general sessions - so more than one user can have active sessions on a single computer.

When the remote user connects to the accessed computer on the console session, Remote Desktop automatically locks that computer (so no other user can access the applications and files). When you come back to your computer at work, you can unlock it by typing CTRL+ALT+DEL.

6.3.2 Configure the Remote Desktop Connection client

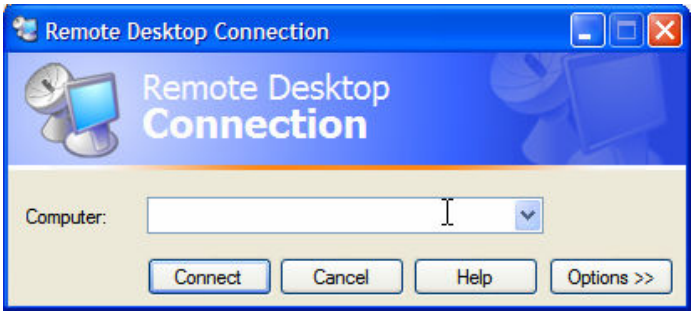
Now you have the Client PC securely connected to the IMG/IM/CM4000 (either locally, or remotely - thru the enterprise VPN, or a secure SSH internet tunnel or a dial-in SSH tunnel) you can establish the Remote Desktop connection from the Client.



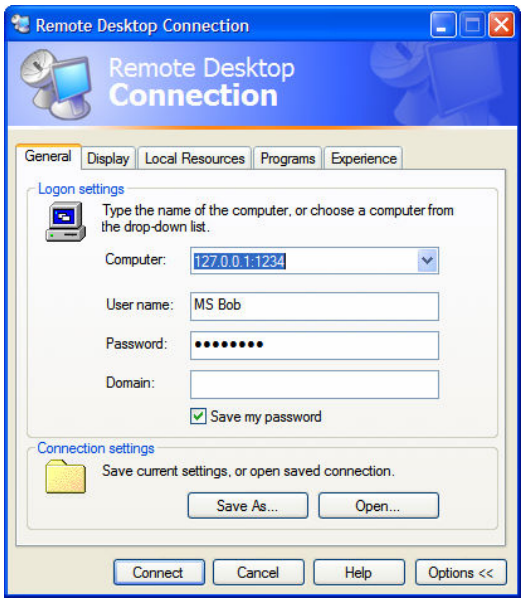
To do this connection you simply enable the **Remote Desktop Connection** on the remote client PC then point it to the SDT Secure Tunnel port in the IMG/IM/CM4000:

A. On a Windows client PC:

- Click **Start**. Point to **Programs**, then to **Accessories**, then **Communications**, and click **Remote Desktop Connection**



- In **Computer**, enter the appropriate IP Address and Port Number:
  - Where there is a direct local or enterprise VPN connection, enter the IP Address of the IMG/IM/CM4000, and the Port Number of the SDT Secure Tunnel for the IMG/IM/CM4000 serial port that is attached to the Windows computer to be controlled e.g. if the Windows computer is connected to serial Port 3 on a IMG/IM/CM4000 located at 192.168.0.50 then you would enter *192.168.0.50:7303*
  - Where there is an SSH tunnel (over a dial up PPP connection or over a public internet connection or private network connection) simply enter the *localhost* as the IP address i.e. *127.0.0.1* For Port Number, enter the *source port* you created when setting SSH tunneling /port forwarding (in Section 6.1.6) e.g. *:1234*
- Click **Option.** In the **Display** section specify an appropriate color depth (e.g. for a modem connection it is recommended you not use over 256 colors). In **Local Resources** specify the peripherals on the remote Windows computer that are to be controlled (printer, serial port etc)



➢ Click **Connect**

Note The Remote Desktop Connection software is pre-installed with Windows XP, however for earlier Windows PCs you will need to download the RDP client:

- Go to the Microsoft Download Center site http://www.microsoft.com/downloads/details.aspx?familyid=80111F21-D48D-426E-96C2-08AA2BD23A49&displaylang=en and click the **Download** button

  This software package will install the client portion of Remote Desktop on Windows 95, Windows 98 and 98 Second Edition, Windows Me, Windows NT 4.0, Windows 2000, and Windows 2003. When run, this software allows these older Windows platforms to remotely connect to a computer running Windows XP Professional or Windows 2003 Server

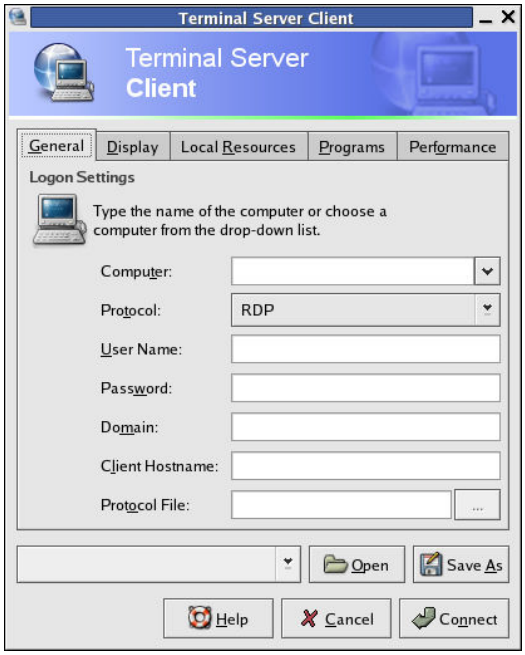
B. On a Linux or UNIX client PC:

➢ Launch the open source *rdesktop* client:

rdesktop -u *windows-user-id* -p *windows-password* -g 1200x950 *ms-windows-terminal-server-host-name*

option	description
-a	Color depth: 8, 16, 24
-r	Device redirection. i.e. Redirect sound on remote machine to local device i.e. -0 -r sound (MS/Windows 2003)
-g	Geometry: *widthxheight* or 70% screen percentage.
-p	Use -p - to receive password prompt.

- You can use GUI front end tools like the GNOME Terminal Services Client *tsclient* to configure and launch the *rdesktop* client. (Using *tsclient* also enables you to store multiple configurations of *rdesktop* for connection to many servers)



Note The *rdesktop* client is supplied with Red Hat 9.0:

- rpm -ivh rdesktop-1.2.0-1.i386.rpm

For Red Hat 8.0 or other distributions of Linux; download source, untar, configure, make, make then install.

rdesktop currently runs on most UNIX based platforms with the X Window System and can be downloaded from http://www.rdesktop.org/

C. On a Macintosh client:

- Download Microsoft's free Remote Desktop Connection client for Mac OS X http://www.microsoft.com/mac/otherproducts/otherproducts.aspx?pid=remotedesktopclient

6.4 SDT Secure Tunnel for VNC

Alternately, with SDT and Virtual Network Computing (VNC), Users and Administrators can securely access and control Windows 98/NT/2000/XP/2003, Linux, Macintosh, Solaris and UNIX computers. There's a range of popular VNC software available (UltraVNC, RealVNC, TightVNC) - freely and commercially.

To set up a secure VNC connection you must install and configure the VNC Server software on the computer to be accessed, then install and configure the VNC Viewer software on the Viewer PC.

6.4.1 Install and configure the VNC Server on the computer to be accessed

Virtual Network Computing (VNC) software enables users to remotely access computers running Linux, Macintosh, Solaris, UNIX, all versions of Windows and most other operating systems.

A. For Microsoft Windows servers (and clients):

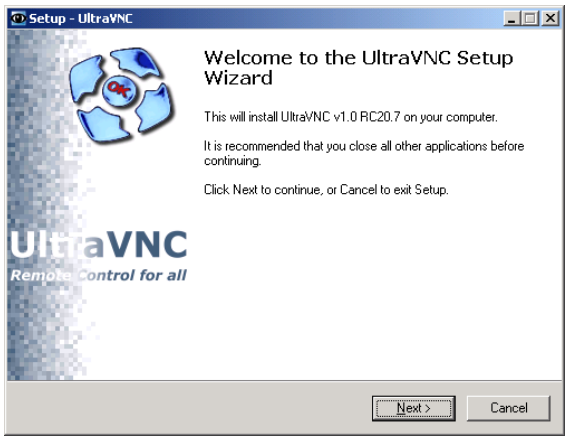
   Windows does not include VNC software, so you will need to download, install and activate a third party VNC Server software package:

RealVNC http://www.realvnc.com is fully cross-platform, so a desktop running on a Linux machine may be displayed on a Windows PC, on a Solaris machine, or on any number of other architectures. There is a Windows server, allowing you to view the desktop of a remote Windows machine on any of these platforms using exactly the same viewer. RealVNC was founded by members of the AT&T team who originally developed VNC.

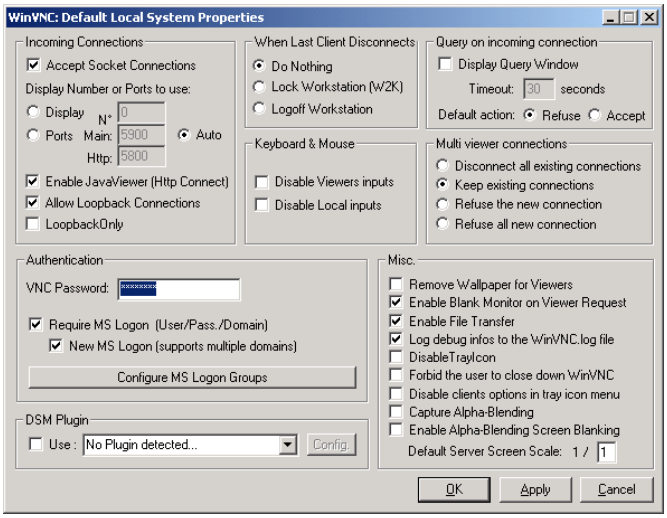
TightVNC http://www.tightvnc.com is an enhanced version of VNC. It has added features such as file transfer, performance improvements, and read-only password support. They have just recently included a video drive much like UltraVNC. TightVNC is still free, cross-platform (Windows Unix and Linux) and compatible with the standard (Real) VNC.

UltraVNC http://ultravnc.com is easy to use, fast and free VNC software that has pioneered and perfected features that the other flavors have consistently refused or been very slow to implement for cross platform and minimalist reasons. UltraVNC runs under Windows operating systems (95, 98, Me, NT4, 2000, XP, 2003) Download UltraVNC from Sourceforge's UltraVNC file list

So, for example, to install and configure the UltraVNC Server on Windows computer, you first select a language (e.g. English) then use the **Set Up** wizard to install the Server software:



Configuring the UltraVNC Server Refer is equally straightforward (though you should refer to http://doc.uvnc.com for more detailed Server (and Viewer) instructions)

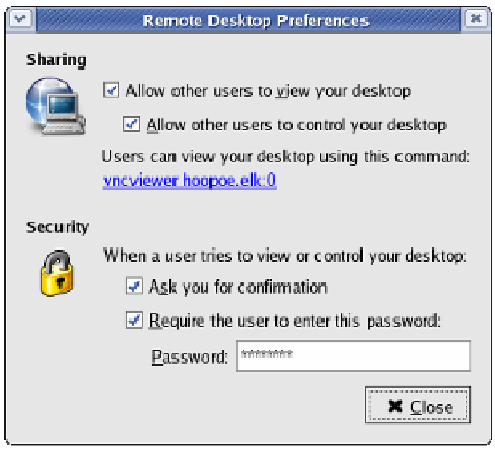


B. For Linux servers (and clients):

Most Linux distributions now include VNC Servers and Viewers and they are generally can be launched from the (Gnome/KDE etc) front end

e.g. with Red Hat Enterprise Linux 4 there's VNC Server software and a choice of Viewer client software, and to launch:

- Select the **Remote Desktop** entry in the **Main Menu -> Preferences** menu
- Click the **Allow other users…** checkbox to allow remote users to view and control your desktop



- To set up a persistent VNC server on Red Hat Enterprise Linux 4:
  - Set a password using **vncpasswd**
  - Edit **/etc/sysconfig/vncservers**
  - Enable the service with **chkconfig vncserver on**
  - Start the service with **service vncserver start**
  - Edit **/home/*username*/.vnc/xstartup** if you want a more advanced session than just *twm* and an xterm

C. For Macintosh servers (and clients):

OSXvnc http://www.redstonesoftware.com/vnc.html is a robust, full-featured VNC server for Mac OS X that allows any VNC client to remotely view and/or control the Mac OS X machine. OSXvnc is supported by Redstone Software

D. Most other operating systems (Solaris, HPUX, PalmOS etc) either come with VNC bundled, or have third party VNC software that you can download.

6.4.2 Install, configure and connect the VNC Viewer

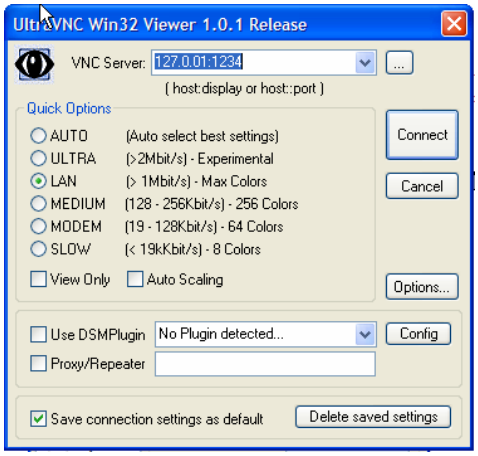
VNC is truly *platform-independent* so a VNC Viewer on any operating system can connect to a VNC Server on any other operating system. There are Viewers (and Servers) from a wide selection of sources (e.g. UltraVNC TightVNC or RealVNC) for most operating systems. There are also a wealth of Java viewers available so that any desktop can be viewed with any Java-capable browser (http://en.wikipedia.org/wiki/VNC lists many of the VNC Viewers sources).

- Install the VNC Viewer software and set it up for the appropriate speed connection

> Note To make VNC faster, when you set up the Viewer:
>
> - Set encoding to ZRLE (if you have a fast enough CPU)
> - Decrease color level (e.g. 64 bit)
> - Disable the background transmission on the Server or use a plain wallpaper
>
> (Refer to http://doc.uvnc.com for detailed configuration instructions)

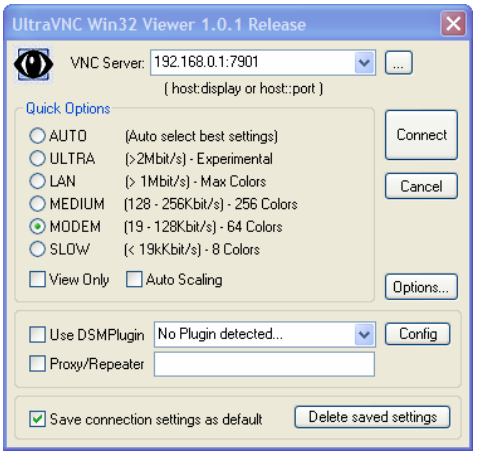
- To establish the VNC connection, first configure the VNC Viewer, entering the VNC Server IP address

A. When the Viewer PC is connected to the IMG/IM/CM4000 thru a SSH tunnel (over the public Internet, or a dial-in connection, or private network connection), enter *locahost* (or 127.0.0.1) as the IP VNC Server IP address; and *the source port* you entered when setting SSH tunneling /port forwarding (in Section 6.2.6) e.g. *:1234*

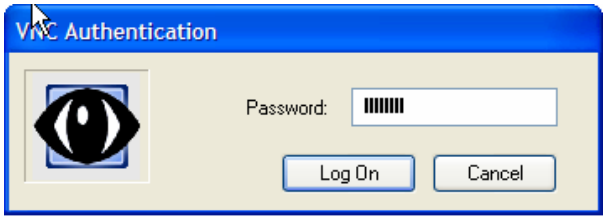


B. When the Viewer PC is connected directly to the IMG/IM/CM4000 (i.e. locally or remotely through a VPN or dial in connection); and the VNC Host computer is serially connected to the CM400; enter the IP address of the IMG/IM/CM4000 unit with the TCP port that the SDT tunnel will use. The TCP port will be 7900 plus the physical serial port number (*i.e.* 7901 to 7948, so all traffic directed to port 79xx on the IMG/IM/CM4000 is tunneled thru to port 5900 on the PPP connection on serial Port xx)

   e.g. for a Windows Viewer PC using UltraVNC connecting to a VNC Server which is attached to Port 1 on a IMG/IM/CM4000 located 192.168.0.1



- You can then establish the VNC connection by simply activating the VNC Viewer software on the Viewer PC and entering the password



Note For general background reading on Remote Desktop and VNC access we recommend the following:

- *The Microsoft Remote Desktop How-To* http://www.microsoft.com/windowsxp/using/mobility/getstarted/remoteintro.mspx
- *The Illustrated Network Remote Desktop* help page http://theillustratednetwork.mvps.org/RemoteDesktop/RemoteDesktopSetupandTroubleshooting.html
- *What is Remote Desktop in Windows XP and Windows Server 2003?* by Daniel Petri http://www.petri.co.il/what's_remote_desktop.htm
- *Frequently Asked Questions about Remote Desktop* http://www.microsoft.com/windowsxp/using/mobility/rdfaq.mspx
- *Secure remote access of a home network using SSH, Remote Desktop and VNC for the home user* http://theillustratednetwork.mvps.org/RemoteDesktop/SSH-RDP-VNC/RemoteDesktopVNCandSSH.html
- *Taking your desktop virtual with VNC,* Red Hat magazine http://www.redhat.com/magazine/006apr05/features/vnc/ and http://www.redhat.com/magazine/007may05/features/vnc/
- *Wikipedia* general background on VNC http://en.wikipedia.org/wiki/VNC

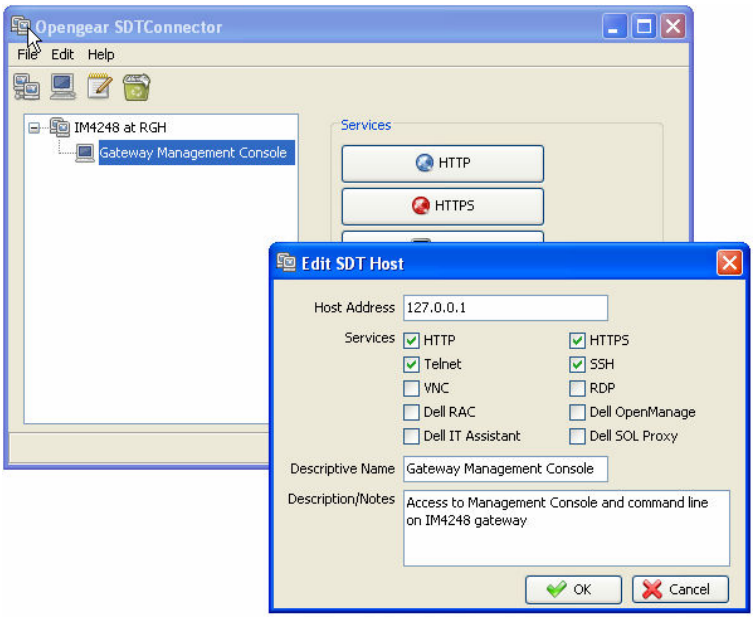
6.5 SDTConnector - browser accessing Management Console

SDT secure tunneling supports remote HTTP/HTTPS access to network devices (like firewalls, routers, power switches) and to monitoring equipment (like electricity/gas service meters, health monitors) that have web browser control interfaces. These appliances or computers are located on the same local network as the IMG/IM/CM4000, and the remote user then connects to the IMG/IM/CM4000 thru an SSH tunnel using *SDTConnector.*

SDTConnector can also be configured for browser access the gateway's Management Console – and for Telnet or SSH access to the gateway command line.

For these connections to the gateway itself, you must configure *SDTConnector* to access the gateway (itself) by setting the IMG/IM/CM4000 gateway up as a *host*, and then configuring the appropriate services:

- Launch *SDTConnector* on your PC. Assuming you have already set up the IMG/IM/CM4000 as a *Gateway* in your *SDTConnector* client (with *username/ password* etc as detailed in Chapter 3.1), select this newly added *Gateway* and click the Host icon to create a host. Alternatively, select **File -> New Host**
- Enter 127.0.0.1 as the **Host Address** and give some details in **Descriptive Name/Notes**. Click OK



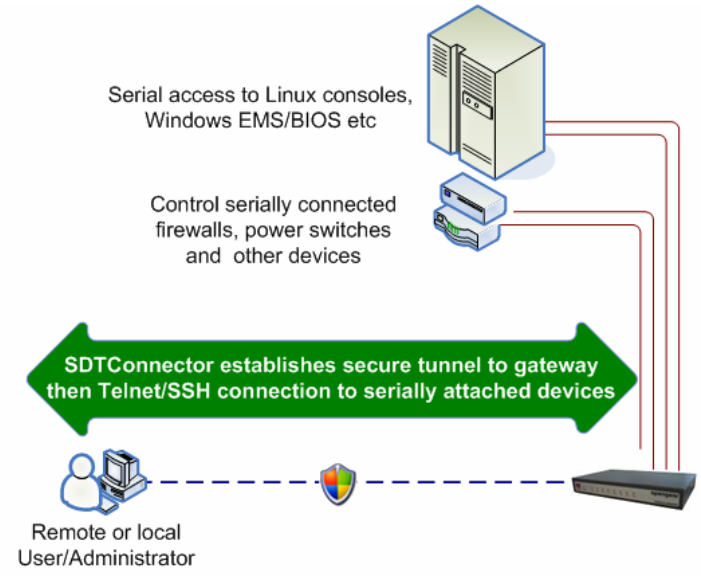
- Click the **HTTP** or **HTTPS** Services icon to access the gateway's Management Console, or click **SSH** or **Telnet** to access the gateway command line console

To enable SDT access to the gateway console, you must now configure the IMG/IM/CM4000 to allow port forwarded network access to itself:

- Browse to the IMG/IM/CM4000 gateway and select **Network Hosts** from **Serial & Network**
- Click **Add Host** and in the **IP Address/DNS Name** field enter 127.0.0.1 (this is the Opengear's network loopback address) and enter *Loopback* in **Description**
- Remove all entries under **Permitted Services** except for those that will be used in accessing the Management Console (80/http or 443/https) or the command line (22/ssh or 23/telnet) then scroll to the bottom and click **Apply**
- Administrators by default have gateway access privileges, however for Users to access the gateway Management Console you will need to give those Users the required access privileges. Select **Users & Groups** from **Serial & Network**. Click **Add User**. Enter a **Username**, **Description** and **Password/Confirm**. Select 127.0.0.1 from **Accessible Host**(s) and click **Apply**

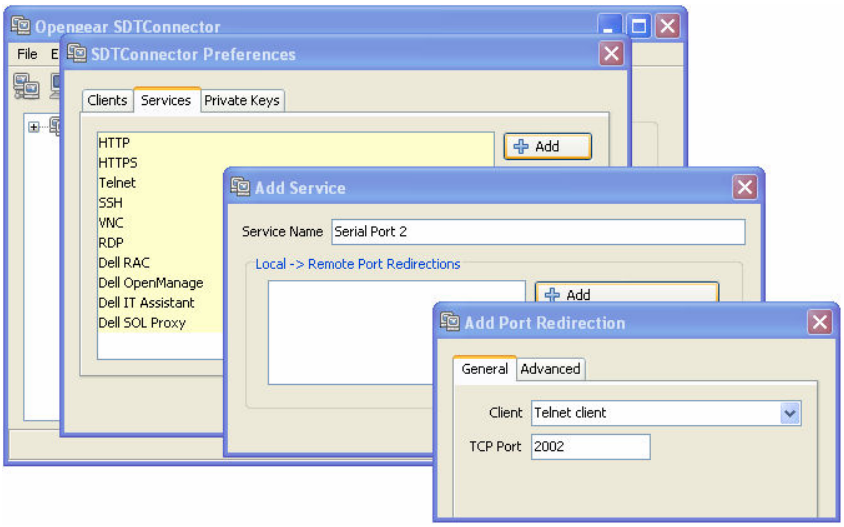
6.6 SDTConnector - Telnet or SSH connection to serially attached devices

SDTConnector can also be used to access text consoles on devices that are attached to the IMG/IM/CM4000 gateway serial ports.



For these connections, you must configure the *SDTConnector* client software with a Service that will access the target gateway serial port, and then set the gateway up as a host:

- Launch *SDTConnector* on your PC. Select **Edit -> Preferences** and click the **Services** tab. Click **Add**
- Enter *"Serial Port 2"* in **Service Name**. Click **Add**
- Select **Telnet** client as the Client. Enter 2002 in **TCP Port**. Click **OK**, then **Close** and **Close** again



- Assuming you have already set up the target IMG/IM/CM4000 as a *gateway* in your *SDTConnector* client (with *username/ password* etc), select this *gateway* and click the **Host** icon to create a host. Alternatively, select **File -> New Host**.
- Enter 127.0.0.1 as the **Host Address** and select **Serial Port 2** for Service. In **Descriptive Name**, enter something along the lines of Loopback ports, or Local serial ports. Click **OK.**
- Click *Serial Port 2* icon for Telnet access to the serial console on the device attached to serial port #2 on the gateway

To enable *SDTConnector* to access to devices connected to the gateway's serial ports, you must also configure the IMG/IM/CM4000 gateway itself to allow port forwarded network access to itself, and enable access to the nominated serial port:

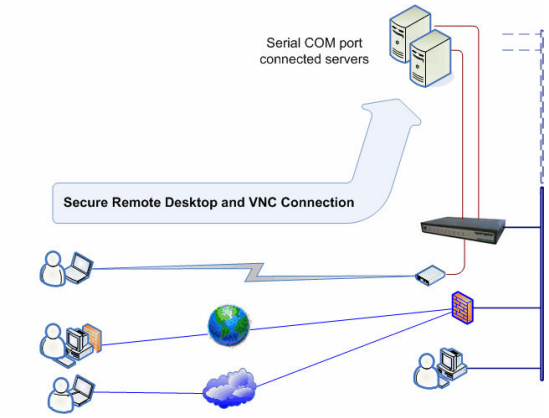
- Browse to the IMG/IM/CM4000 gateway and select **Serial Port** from **Serial & Network**
- Click **Edit** next to selected Port # (e.g. Port 2 if the target device is attached to the second serial port). Ensure the port's serial configuration is appropriate for the attached device
- Scroll down to **Console Server Setting** and select **Console Server Mode**. Check **Telnet** (or SSH) and scroll to the bottom and click **Apply**
- Select **Network Hosts** from **Serial & Network** and click **Add Host**
- In the **IP Address/DNS Name** field enter *127.0.0.1* (this is the Opengear's network loopback address) and enter *Loopback* in **Description**

- Remove all entries under **Permitted Services** and select **TCP** and enter *200n* in **Port**. (This configures the Telnet port enabled in the previous step, so for Port 2 you would enter *2002*)
- Click **Add** then scroll to the bottom and click **Apply**
- Administrators by default have gateway and serial port access privileges; however for Users to access the gateway and the serial port, you will need to give those Users the required access privileges. Select **Users & Groups** from **Serial & Network**. Click **Add User**. Enter a **Username**, **Description** and **Password/Confirm**. Select 127.0.0.1 from **Accessible Host**(s) and select Port 2 from Accessible Port(s). Click **Apply.**

6.7 Using SDT to IP connect to hosts that are serially attached to the gateway

Network (IP) protocols like RDP, VNC and HTTP can be used for connecting to host devices that are serially connected through their COM port to the IMG/IM/CM4000. To do this you must:

- establish a PPP connection (Section 6.7.1) between the host and the gateway, then
- set up Secure Tunneling - Ports on the IMG/IM/CM4000 (Section 6.7.2), then
- configure *SDTConnector* to use the appropriate network protocol to access IP consoles on the host devices that are attached to the IMG/IM/CM4000 gateway serial ports (Section 6.7.3).



6.7.1 Establish a PPP connection between the host COM port and IMG/IM/CM4000

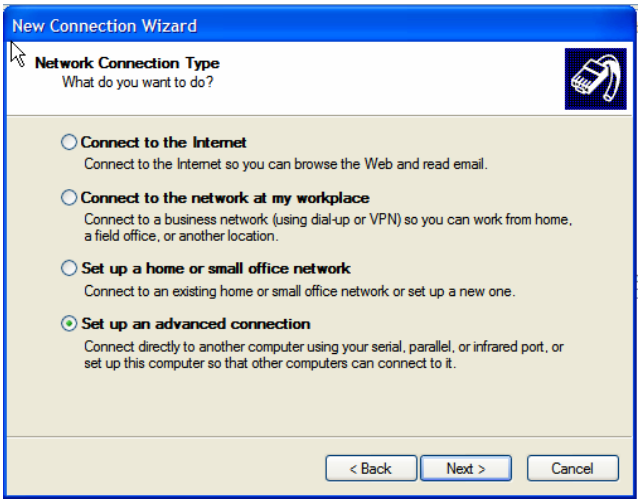
(This step is only necessary for serially connected computers)

Firstly, physically connect the COM port on the host computer that is to be accessed, to the serial port on the IMG/IM/CM4000 then:

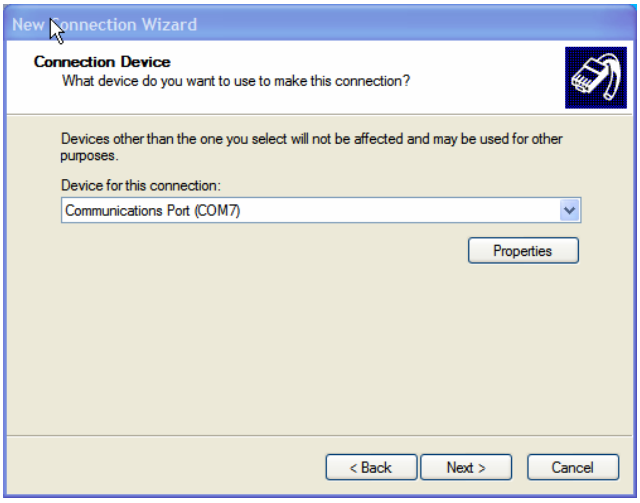
A. For non Windows (Linux, UNIX, Solaris etc) computers establish a PPP connection over the serial port. The online tutorial http://www.yolinux.com/TUTORIALS/LinuxTutorialPPP.html presents a selection of methods for establishing a PPP connection for Linux

B. For Windows XP and 2003 computers follow the steps below to set up an advanced network connection between the Windows computer, through its COM port to the IMG/IM/CM4000. Both Windows 2003 and Windows XP Professional allow you to create a *simple dial in service* which can be used for the Remote Desktop/VNC/HTTP/X connection to the IMG/IM/CM4000:

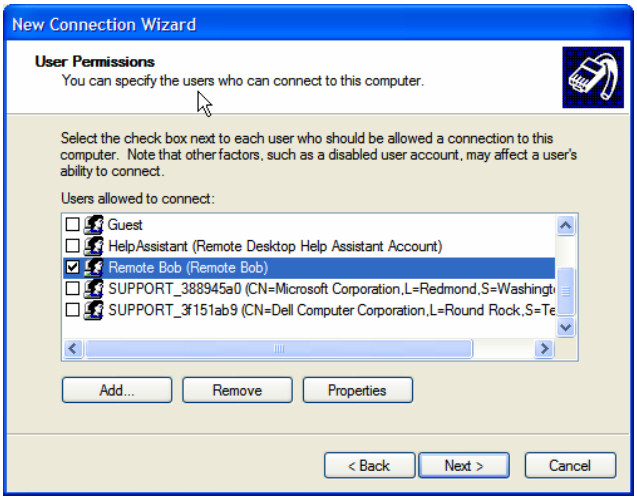
- Open **Network Connections** in Control Panel and click the **New Connection Wizard**



- Select **Set up an advanced connection** and click **Next**
- On the **Advanced Connection Options** screen select **Accept Incoming Connections** and click **Next**

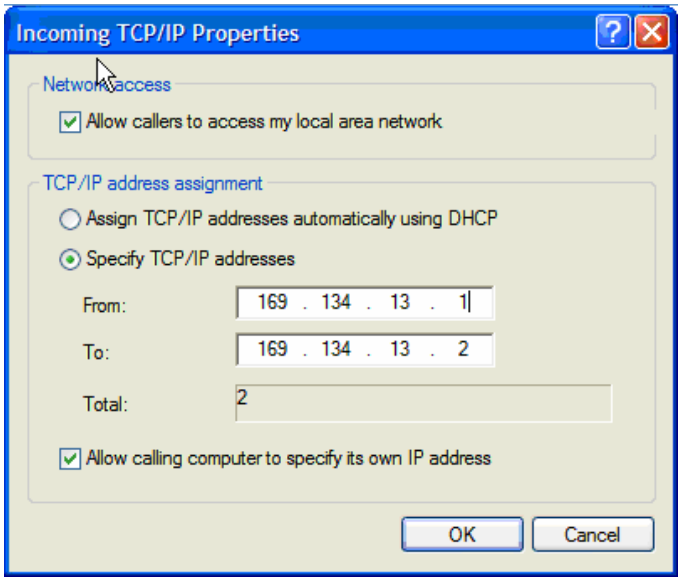


- Select the **Connection Device** (i.e. the serial COM port on the Windows computer that you cabled through to the IMG/IM/CM4000). By default select **COM1**. The COM port on the Windows computer should be configured to its maximum baud rate. Click **Next**
- On the **Incoming VPN Connection Options** screen select **Do not allow virtual private connections** and click **Next**



- Specify which Users will be allowed to use this connection. This should be the same Users who were given Remote Desktop access privileges in the earlier step. Click **Next**

- On the **Network Connection** screen select **TCP/IP** and click **Properties**



- Select **Specify TCP/IP addresses** on the **Incoming TCP/IP Properties** screen select **TCP/IP.** Nominate a *From:* and a *To:* TCP/IP address and click **Next**

Note You can choose any TCP/IP addresses so long as they are addresses which are not used anywhere else on your network. The *From:* address will be assigned to the Windows XP/2003 computer and the *To:* address will be used by the IMG/IM/CM4000.

For simplicity use the IP address as shown in the illustration above:

From: 169.134.13.1
To: 169.134.13.2

Alternately you can set the advanced connection and access on the Windows computer to use the IMG/IM/CM4000 defaults:

- Specify 10.233.111.254 as the *From:* address
- Select *Allow calling computer to specify its own address*

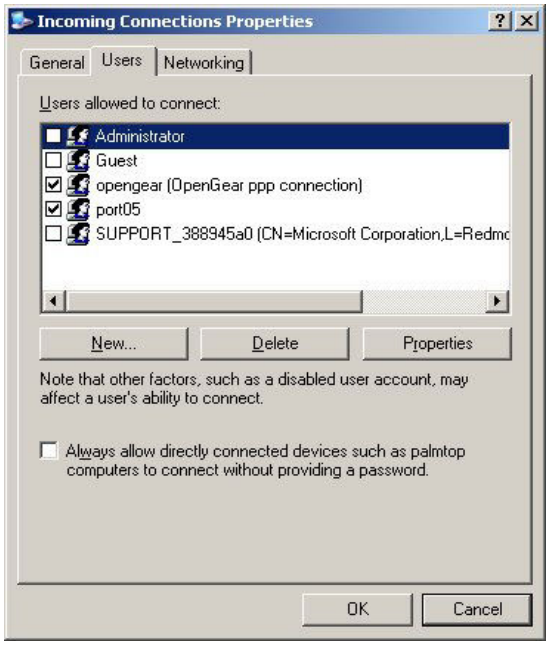
Also you could use the IMG/IM/CM4000 default username and password when you set up the new Remote Desktop User and gave this User permission to use the advance connection to access the Windows computer:

- The IMG/IM/CM4000 default *Username is portXX* where XX is the serial port number on the IMG/IM/CM4000.
- The default *Password is portXX*

So to use the defaults for a RDP connection to the serial port 2 on the IMG/IM/CM4000, you would have set up a Windows user named *port02*

- When the PPP connection has been set up, a network icon will appear in the Windows task bar

Note The above notes describe setting up an incoming connection for Windows XP. The steps are the same for Windows 2003, except that the set up screens present slightly differently:



You need to put a check in the box for *Always allow directly connected devices such as palmtop…..*

Also the option for to **Set up an advanced connection** is not available in Windows 2003 if RRAS is configured. If RRAS has been configured it is a simply task to enable the null modem connection for the dial-in configuration.

C. For earlier version Windows computers again follow the steps in Section B. above, however to get to the **Make New Connection** button:

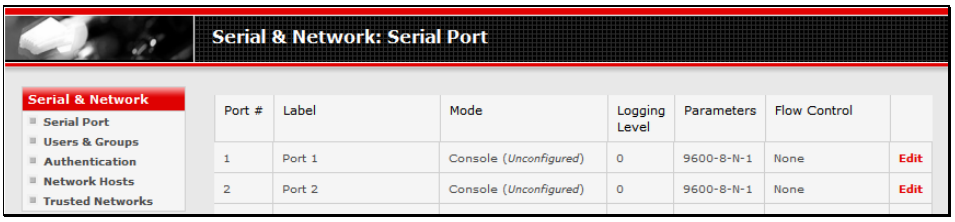
- For Windows 2000, click **Start** and select **Settings** then at the **Dial-Up Networking Folder** click **Network and Dial-up Connections** and click **Make New Connection.** Note you may need to first set up connection over the COM port using **Connect directly to another computer** before proceeding to **Set up an advanced connection**

- For Windows 98 you double click **My Computer** on the Desktop, then open **Dial-Up Networking** and double click

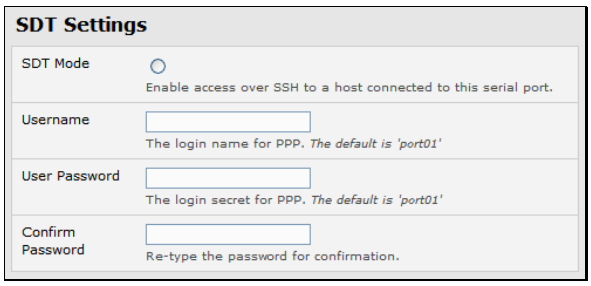
6.7.2 Set up SDT Serial Ports on IMG/IM/CM4000

To set up *RDP (and VNC) forwarding* on the IMG/IM/CM4000 Serial Port that is connected to the Windows computer COM port:

- Select the **Serial & Network: Serial Port** menu option and click **Edit** (for the particular Serial Port that is connected to the Windows computer COM port)



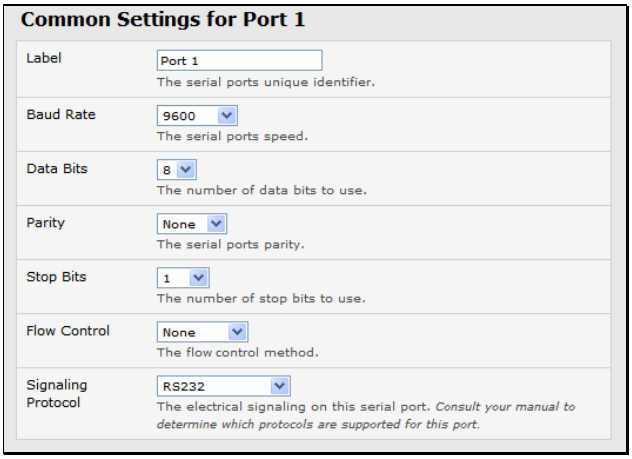
- On the SDT Settings menu select **SDT Mode** (which will enable port forwarding and SSH tunneling) and enter a **Username** and **User Password.**



Note When you enable SDT, this will override all other Configuration protocols on that port

Note If you leave the *Username* and *User Password* fields blank, they default to *portXX* and *portXX* where XX is the serial port number. So the default username and password for Secure RDP over Port 2 is *port02*

- Ensure the IMG/IM/CM4000 **Common Settings** (Baud Rate, Flow Control) are the same as were set up on the Windows computer COM port and click **Apply**



- RDP and VNC forwarding over serial ports is enabled on a Port basis. You can add Users who can have access to these ports (or reconfigure User profiles) by selecting **Serial & Network :User & Groups** menu tag - as described earlier in Chapter 4 *Configuring Serial Ports*

6.7.3 Set up SDTConnector to ssh port forward over the IMG/IM/CM4000 Serial Port

In the *SDTConnector* software running on your remote computer specify the gateway IP address of your CM4000 and a username/password for a user you have setup on the CM4000 that has access to the desired port. You can refer to page 46 of the manual for help on configuring users on the CM4000.

Next you need to add a New SDT Host. In the Host address you need to put portxx where xx = the port you are connecting to. Example for port 3 you would have a Host Address of: port03

Select the RDP Service check box.

That should work for you. I threw these instructions together quickly, so if something does not make sense to you please let us know. And if it is still not working can you send us a copy of your syslog after attempting to connect?

Chapter 7 Alerts and Logging

Introduction

This chapter describes the logging and alert generation features of the gateway. Port logging can maintain a record of all access and communications with the IMG/IM/CM4000 and with the attached serial devices. The IM42XX also logs access and communications with network attached hosts:

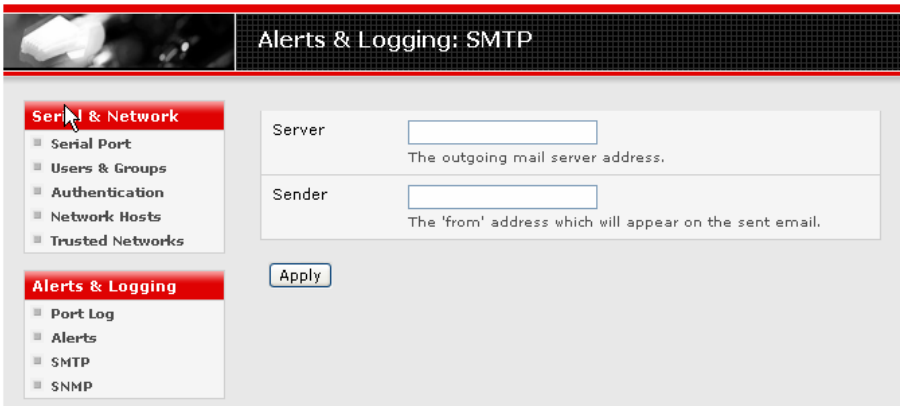
- First you must set up the destination to which any Alert (which may result from monitoring serial and network port access and traffic) is to be sent
- If port logs are to be maintained on a remote server, then the access path to this location need to be configured
- Then you need to activate and set the desired levels of logging for each serial and/or network port
- The Alert facility monitors the ports and emails alerts when specified activity events occur
- A log of all system activity is also maintained

7.1 SMTP and SNMP Settings

With the Alerts facility enabled the nominated ports/hosts are monitored for trigger conditions. When triggered, an Alert message is emailed to a nominated email address (SMTP), or sent to a designated SNMP destination. Before setting up the alert trigger, you must specify the alert destination.

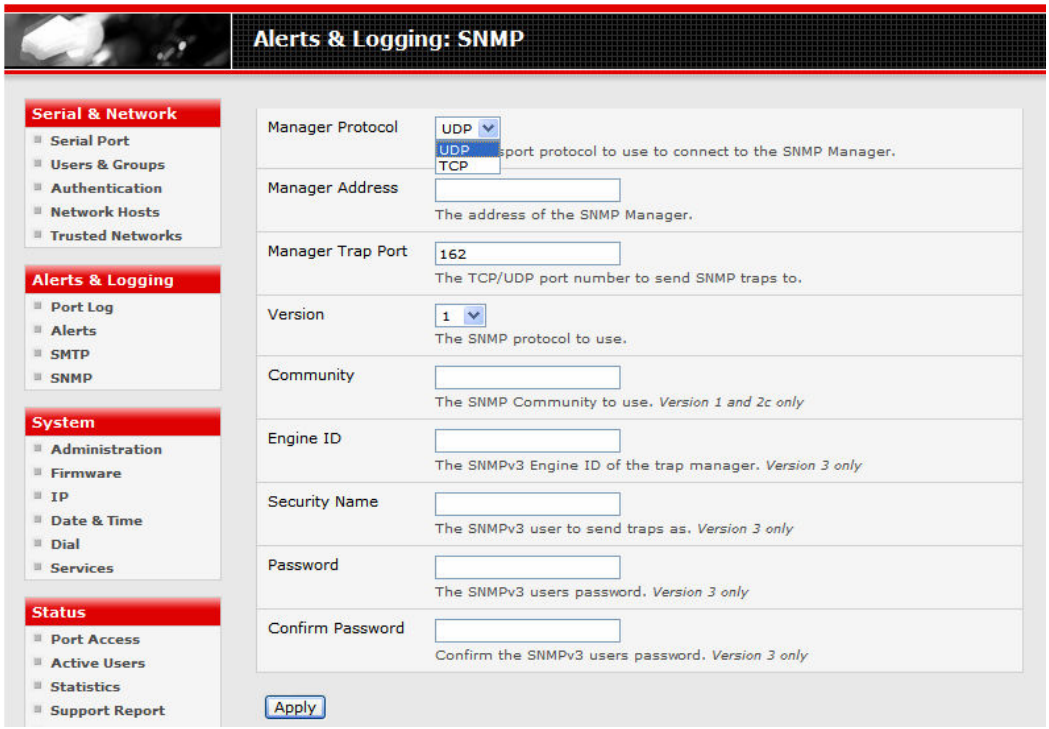
To set up the email alert destination:

- Select **Alerts & Logging: SMTP** and in the **Server** field enter the IP address of the outgoing mail server
- You may optionally enter an **Sender** email address which will appear as the *from* address in all sent email from this IMG/IM/CM4000
- Click **Apply** to activate SMTP



To set up SNMP alert destination:

- Select **Alerts & Logging: SNMP** and specify the SNMP management destination server and protocols, and configure access security.

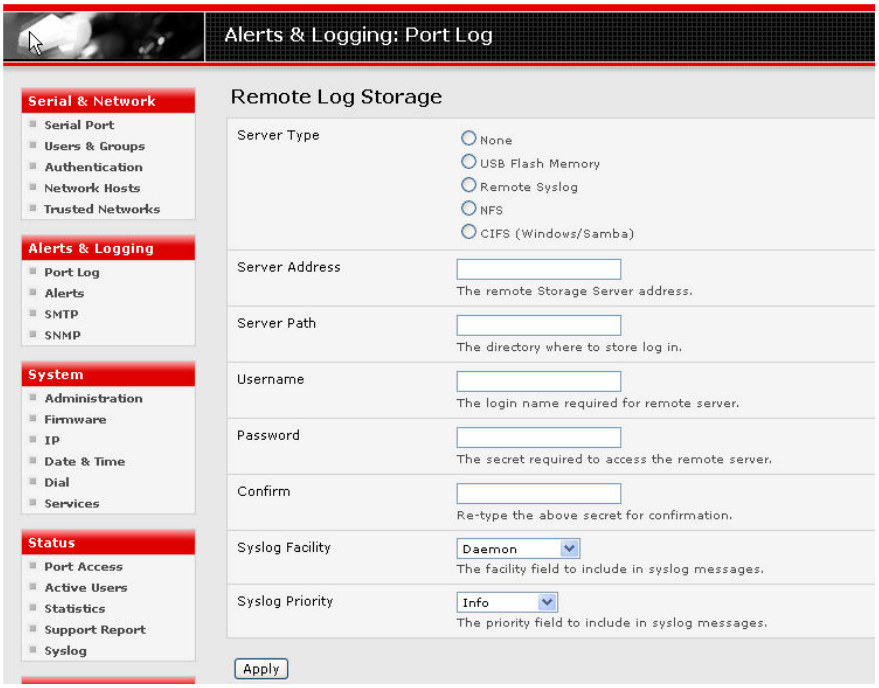


- Click **Apply** to activate SNMP

7.2 Remote Log Storage

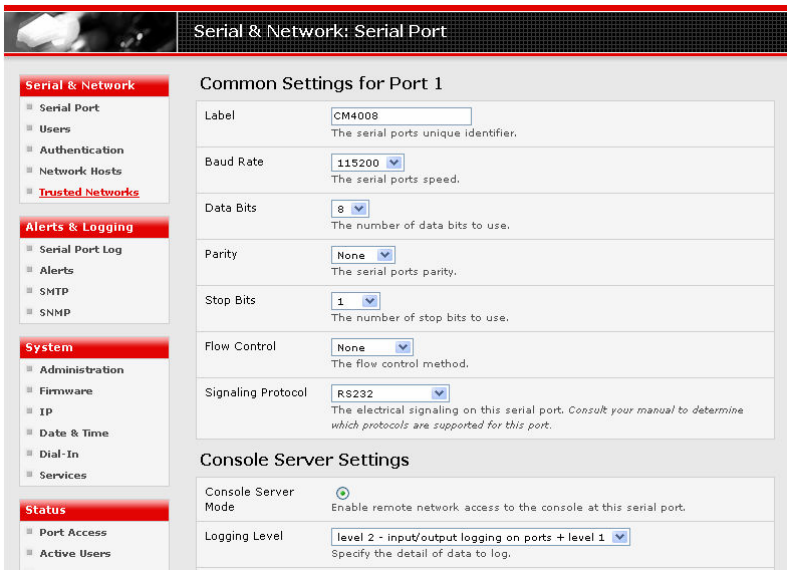
Before activating Serial or Network Port Logging on any port, you must specify where those logs are to be saved:

- Select the **Alerts & Logging: Port Log** menu option and specify the **Server Type** to be used, and the details to enable log server access



7.3 Serial Port Logging

In Console Server mode, activity logs can be maintained of all serial port activity. These records are stored on an off-server, or in the IM/IMG gateway flash memory. To specify which serial ports are to have activities recorded and to what level data is to be logged:



- Select **Serial & Network: Serial Port** and **Edit** the port to be logged
- Specify the **Logging Level** of for each port as:

  Level 0 Turns off logging for the selected port

  Level 1 Logs all connection events to the port

  Level 2 Logs all data transferred to and from the port and all changes in hardware flow control status and all User connection events

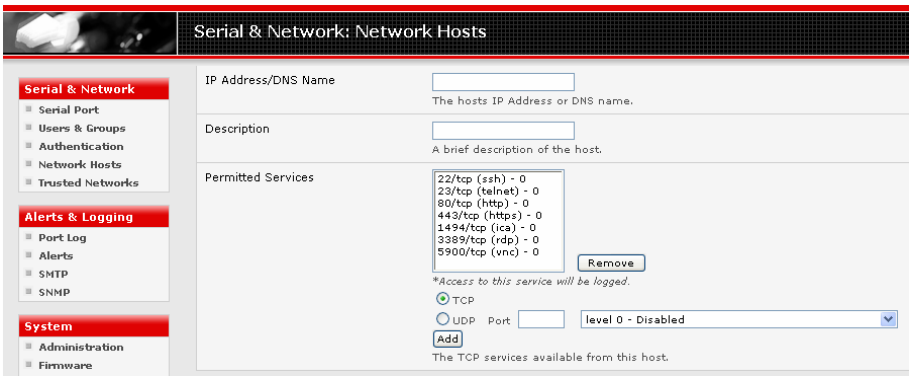
- Click **Apply**

Note A cache of the most recent 8K of logged data per serial port is maintained locally (in addition to the Logs which are transmitted for remote/USB flash storage). To view the local cache of logged serial port data select **Manage: Port Logs**

7.4 Network TCP or UDP Port Logging (IMG4xxx and IM42xx only)

The IM42XX products support optional logging of access to and communications with network attached Hosts.

- For each Host, when you set up the Permitted Services which are authorized to be used, you also must set up the level of logging that is to be maintained for each service.



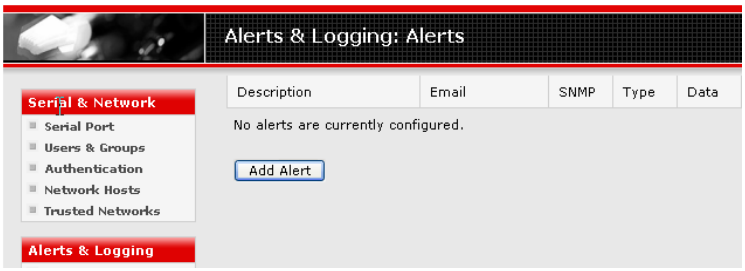
- Specify the logging level that is to be maintained for that particular TDC/UDP port/service, on that particular Host:

Level 0	Turns off logging for the selected TDC/UDP port to the selected Host
Level 1	Logs all connection events to the port
Level 2	Logs all data transferred to and from the port and all changes in hardware flow control status and all User connection events

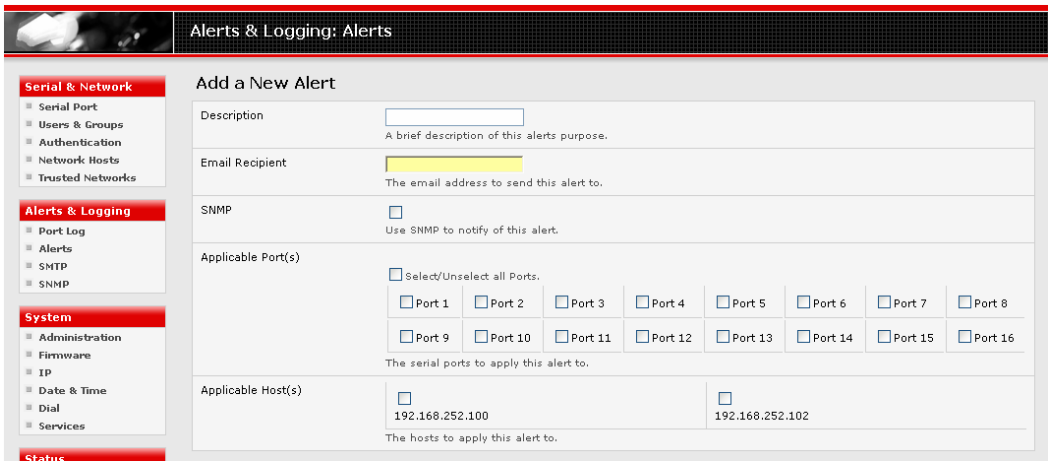
- Click **Add** then click **Apply**

7.5 Configure Port Alerts

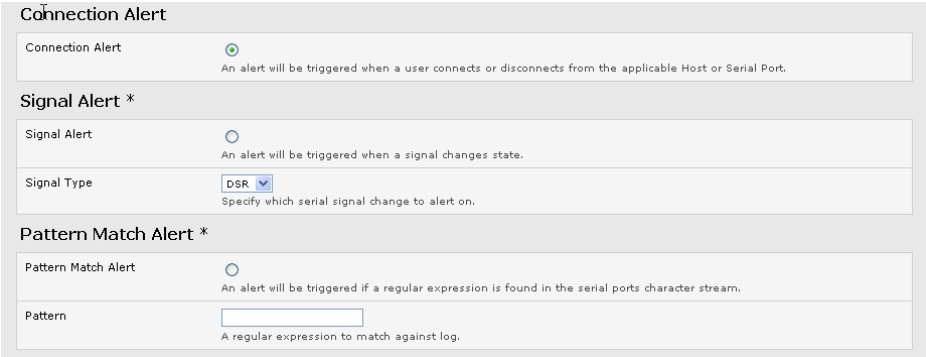
The Alerts facility enables the data stream from a nominated serial port to be monitored for trigger conditions. User connections to serial ports and Hosts can also be a trigger event. When triggered, an Alert message is then emailed to a nominated email address, or an SNMP server is notified.



- Select **Alerts & Logging: Alerts** and click **Add Alert**



- At **Add a New Alert** enter a description for the alert/trigger condition and select which the serial ports and/or Hosts are to be monitored for this alert trigger
- Nominate the email address for the **Email Recipient** who will be notified of the alert, and/or activate **SNMP** notification for this event



- Select the Alert Type (**Connection**, **Signa**l or **Pattern Match**). Signal and Pattern Match alerts are applicable to serial ports only.
- If Signal or Pattern Match alerts were selected you must also specify the particular **Signal Type** or **Pattern** trigger condition that will send a new alert. You can configure a selection of different Alert types and any number of specific Alert triggers for each serial port
- Click **Apply**

Chapter 8 Power Control

Introduction

Users and Administrators can use their IMG/IM/CM4000 gateways to remotely power on, power off, power cycle and read the current status of power strips, UPS supplies and servers:

- Serial port controlled power strips can be controlled by using their command line console as detailed in *Chapter 4.* However these serial port controlled power strips can also be securely accessed and controlled using the Management Console's power control tools – as covered in this chapter

- Network-attached power strips with browser controls can be controlled by directly sending HTTP/HTTPS commands with SDT as detailed in *Chapter 6.3*. Alternately these browser controlled power strips can be securely accessed and controlled using the Management Console's power control tools – again as covered in this chapter

- Servers and network-attached appliances with embedded IPMI service processors or BMCs invariably are supplied with their own management tools (like SoL) that will provide secure management when connected using with SDT. These IPMI controlled power switches can also be controlled using the Management Console's power control tools – as covered in this chapter

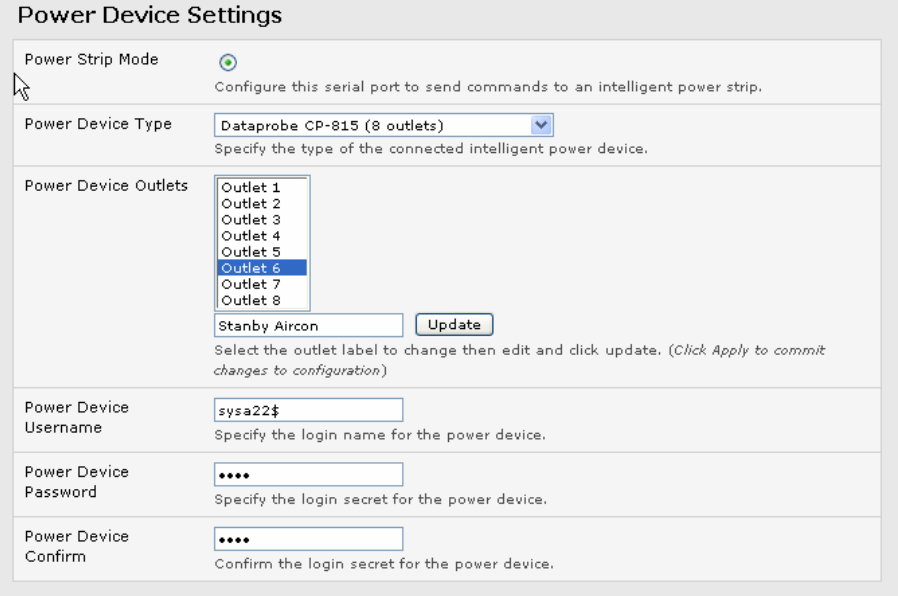
- And servers with embedded service processors (like Dell's DRAC) usually provide power control using the browser based management applications that are supplied with the service processor (like Dell's Open Manage) – and these applications invariably can be connected (securely in and out-of-band) using SDT

8.1 Configuring Serial Port Power Strips

The Administrator can configure serially connected power strips, so both Users and Administrators can control them directly using the Management Console. First the selected gateway serial port must be connected to, and configured to communicate with the power strip:

- Connect the power strip to the selected serial port on the IMG/IM/CM4000 gateway

- Select the **Serial and Network: Serial** menu option and configure the **Common Settings** of selected gateway serial port that will be connected to the power strip with the RS232 properties etc required by the power strip (refer *Chapter 4.1.1 Common Settings*)



- Select **Power Strip Mode,** then select the **Power Device Type** to be controlled

- To simplify power management, you also can also optionally apply a text label to each of the power outlets on the power strip you have installed

> **Note** The IP Power 9258 is a web controlled device, however it does offer serial control mode for emergency reset. This serial mode enables all the power ports to be powered off /on. Whereas with browser access individual outlets power can be power cycled and power on can be scheduled etc.

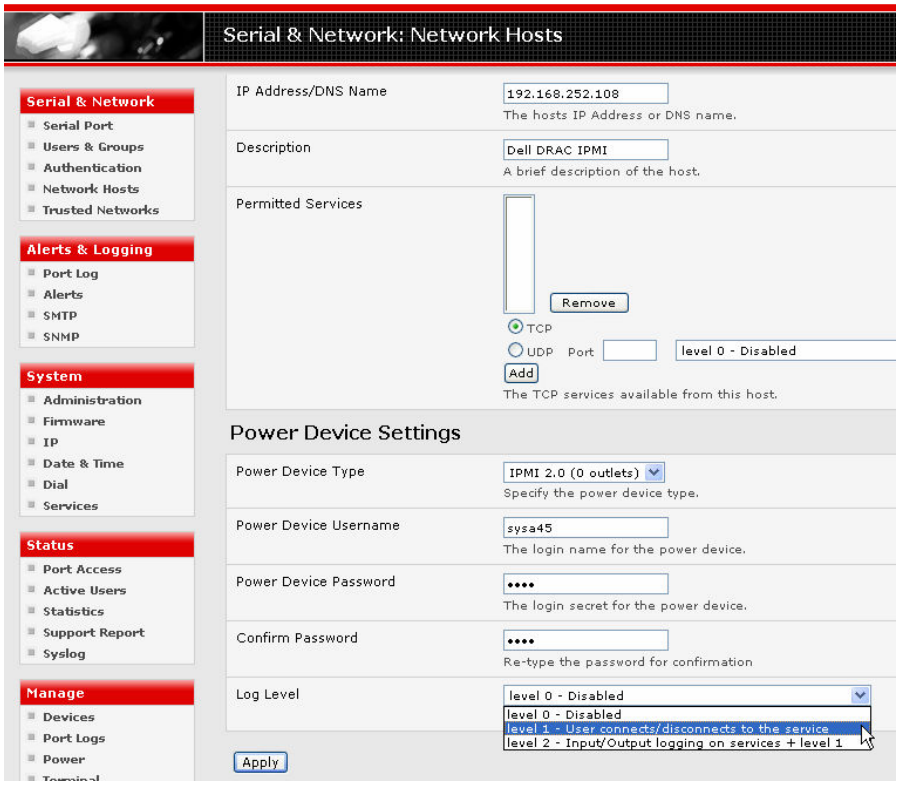
- Enter the **Username** and **Password** for accessing the Power Device

- Click **Apply**

Note The Management Console has support for a number of popular serial power-control devices. If your device is not on the default list it is simple to add support for more devices, and this is covered in Chapter 14 - Advanced Configurations

8.2 Configuring IPMI Power Management

The IMG/IM/CM4000 provides power management of servers, storage and telco devices built with embedded IPMI service processors and BMCs. The Administrator can configure these IPMI devices, so both Users and Administrators can use the Management Console to remotely cycle power and reboot, even when the operating system is unresponsive.

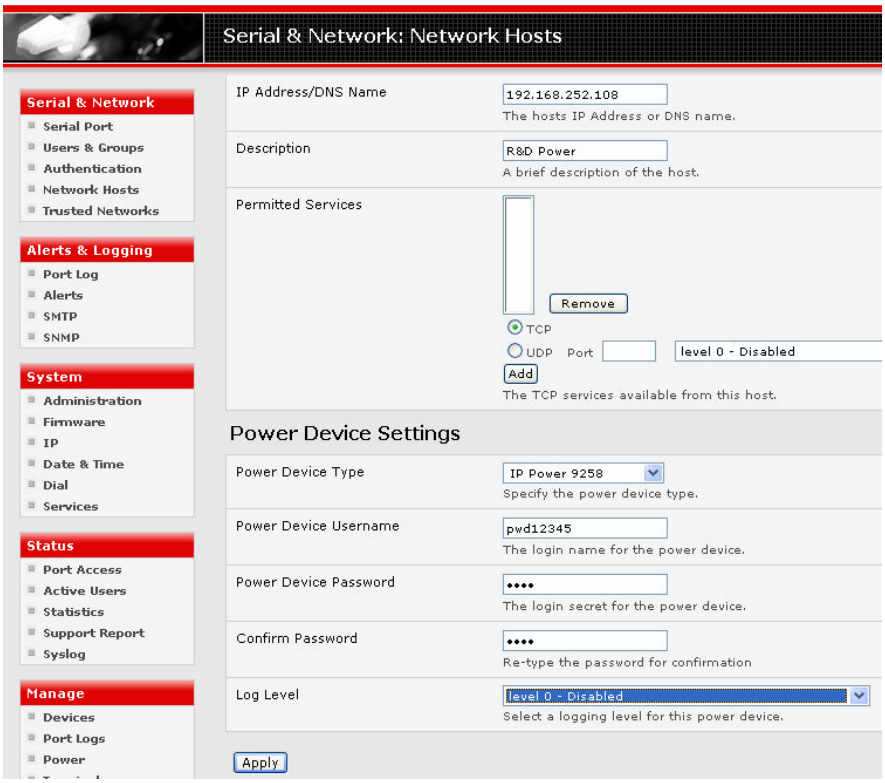


To set up networked server for IPMI power control, the Administrator must configure the embedded IPMI device to communicate:

- Select **Serial & Network: Network Hosts** and enter the IP Address/Domain Name of the BMC or Service Processor (e.g. Dell DRAC)
- Then in **Power Device Settings**, specify the IPMI **Power Device Type** (1.5 or 2.0) and **Username Password**
- For IM42XX you can also select the **Log Level** for logging of all access to this device access (refer Alerts and Logging *Chapter 7*)
- Click **Apply**

8.2 Configuring browser controlled Power Strips

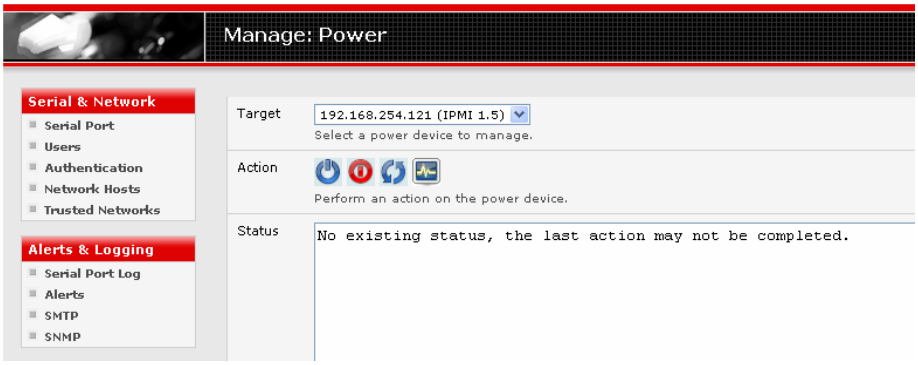
The Administrator can configure network attached power strips, so both Users and Administrators can control them directly using the Management Console.



The Management Console is supplied preconfigured with the HTTP commands for the IP Power 9258 power strip. Is it simple to add support for other browser controlled power devices and this is covered in *Chapter 15 - Advanced Configurations*

8.3 Controlling Power

The Power Manager enables both Users and Administrators to access and control these configured serial and network attached power strips and servers with embedded IPMI service processors or BMCs:



- Select the **Manage: Power** and the particular **Target** power device to be controlled
- Then initiate the desired **Action** to be taken by selecting the appropriate icon:

Power ON

Power OFF

Power Cycle

Power Status

You will only be presented with icons for those operations that are supported by the **Target** you have selected

Chapter 9 Authentication

Introduction

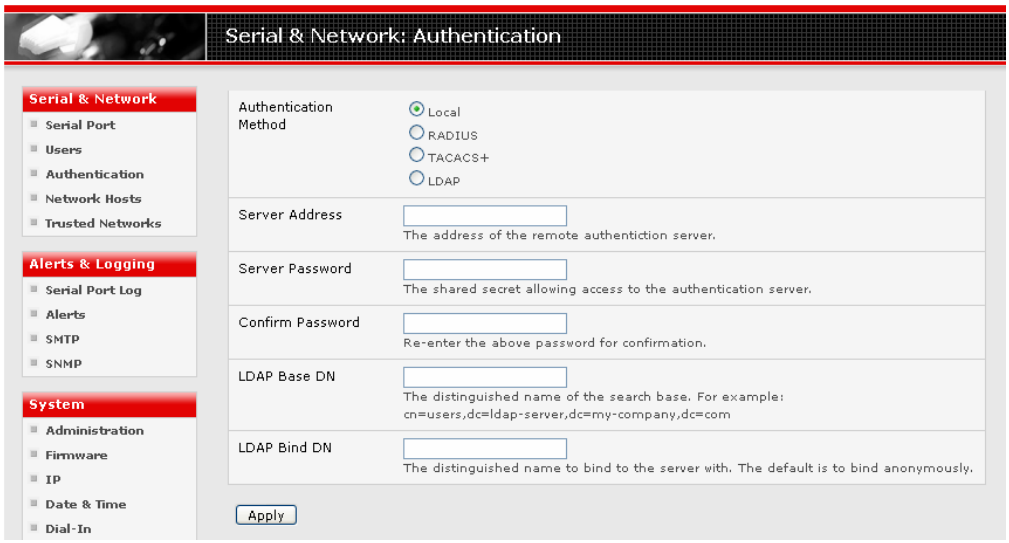
The IMG/IM/CM4000 platform is a dedicated Linux computer, and it embodies a myriad of popular and proven Linux software modules for networking, secure access (OpenSSH) and communications (OpenSSL) and sophisticated user authentication (PAM, RADIUS, TACACS+ and LDAP).

- This chapter details how the Administrator can use the Management Console to establish remote authentication for all User connections to ports on the IMG/IM/CM4000
- This chapter also covers establishing a secure link to the Management Console using HTTPS and using OpenSSL and OpenSSH for establishing secure Administration connection to the IMG/IM/CM4000

9.1 Remote Authentication Configuration

By default all access to the IMG/IM/CM4000 uses local authentication (rather than remote authentication). The Administrator always uses local authentication, whether connected in-band or out-of-band *via* the modem link.

The Administrator can use the Management Console to set up remote authentication for all User connections to ports on the IMG/IM/CM4000. The remote authentication database is then used to verify the username and password received from Users. To enable remote authentication:



- Select **Serial and Network: Authentication**
- Select if **Radius TACAS+** or **LDAP** authentication is to be used. For local authentication only, select **Local**
- Enter the **Server Address** (IP or host name) of the remote authentication server and the **Server Password**
- Click **Apply.** The selected remote authentication will now be used for all user access to gateway ports

RADIUS The Remote Authentication Dial-In User Service (RADIUS) protocol was developed by Livingston Enterprises as an access server authentication and accounting protocol. The RADIUS server can support a variety of methods to authenticate a user. When it is provided with the username and original password given by the user, it can support PPP, PAP or CHAP, UNIX login, and other authentication mechanisms.

TACACS+ The Terminal Access Controller Access Control System (TACACS+) security protocol is a more recent protocol developed by Cisco. It provides detailed accounting information and flexible administrative control over the authentication and authorization processes. TACACS+ allows for a single access control server (the TACACS+ daemon) to provide authentication, authorization, and accounting services independently. Each service can be tied into its own database to take advantage of other services available

on that server or on the network, depending on the capabilities of the daemon. There is a draft RFC detailing this protocol.

LDAP The Lightweight Directory Access Protocol (LDAP) is based on the X.500 standard, but significantly simpler and more readily adapted to meet custom needs. The core LDAP specifications are all defined in RFCs. LDAP is a protocol used to access information stored in an LDAP server.

> **Note** To interact with RADIUS, TACACS+ and LDAP requires that the user account exist on our IM/CM4000 to work with the remote server i.e. You can't just create the user on your RADIUS server and not tell the IM/CM4000 about it. You need to add the user account.

9.2 PAM (Pluggable Authentication Modules)

The IMG/IM/CM4000 supports RADIUS, TACACS+ and LDAP for two-factor authentication *via* PAM (Pluggable Authentication Modules). PAM is a flexible mechanism for authenticating Users. Nowadays a number of new ways of authenticating users have become popular. The problem is that each time a new authentication scheme is developed; it requires all the necessary programs (login, ftpd *etc*.) to be rewritten to support it.

PAM provides a way to develop programs that are independent of authentication scheme. These programs need "authentication modules" to be attached to them at run-time in order to work. Which authentication module is to be attached is dependent upon the local system setup and is at the discretion of the local Administrator.

The IMG/IM/CM4000 family supports PAM to which we have added the following modules for remote authentication:

RADIUS	- pam_radius_auth	(http://www.freeradius.org/pam_radius_auth/)
TACACS+	- pam_tacplus	(http://echelon.pl/pubs/pam_tacplus.html)
LDAP	- pam_ldap	(http://www.padl.com/OSS/pam_ldap.html)

Further modules can be added as required.

For further information on configuring remote RADIUS, TACACS+ or LDAP servers can be found at the following sites:

RADIUS

http://www.microsoft.com/technet/prodtechnol/windowsserver2003/library/DepKit/d4fe8248-eecd-49e4-88f6-9e304f97fefc.mspx

http://www.cisco.com/en/US/tech/tk59/technologies_tech_note09186a00800945cc.shtml

http://www.freeradius.org/

TACACS+

http://www.cisco.com/en/US/tech/tk59/technologies_tech_note09186a0080094e99.shtml

http://www.cisco.com/en/US/products/sw/secursw/ps4911/products_user_guide_chapter09186a00800eb6d6.html

http://cio.cisco.com/univercd/cc/td/doc/product/software/ios113ed/113ed_cr/secur_c/scprt2/sctplus.htm

LDAP

http://www.ldapman.org/articles/intro_to_ldap.html

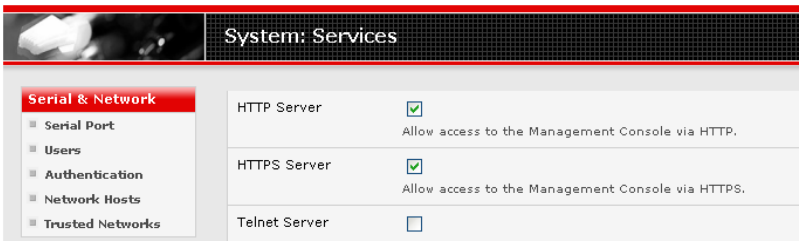
http://www.ldapman.org/servers.html

http://www.linuxplanet.com/linuxplanet/tutorials/5050/1/

http://www.linuxplanet.com/linuxplanet/tutorials/5074/4/

9.3 Secure Management Console Access

If you selected **HTTPS Server** in **Network: Services** then this will enable you, the Administrator, to establish a secure browser connection to the IMG/IM/CM4000 Management Console. To securely access the Management Console from a network connected PC or workstation, you must:



- Activate your preferred browser and enter **https:// IMG/IM/CM4000's IP address** e.g. if the IMG/IM/CM4000 has been set up with an IP address of 200.122.0.12 you need to type https:// 200.122.0.12 in your address bar

- Your browser may respond with a message that verifies the security certificate is valid but notes that it is not necessarily verified by a certifying authority. To proceed you need to click *yes* if you are using Internet Explorer or select *accept this certificate permanently* (or *temporarily*) if you are using Mozilla Firefox.

- You will then be prompted for the Administrator account and password as normal.

When you have a secure HTTPS connection in place the SSL secured icon will appear at the bottom of the browser screen. You can verify the level of encryption in place by clicking on this icon.

When you first enable and connect *via* HTTPS it is normal that you may receive a certificate warning. The default SSL certificate in your IMG/IM/CM4000 is embedded during testing and it is not signed by a recognized third party certificate authority (rather it is signed by our own signing authority). These warnings do not affect the encryption protection you have against eavesdroppers.

Note More detailed information on issuing certificates and configuring HTTPS can be found in Chapter 13 - Advanced

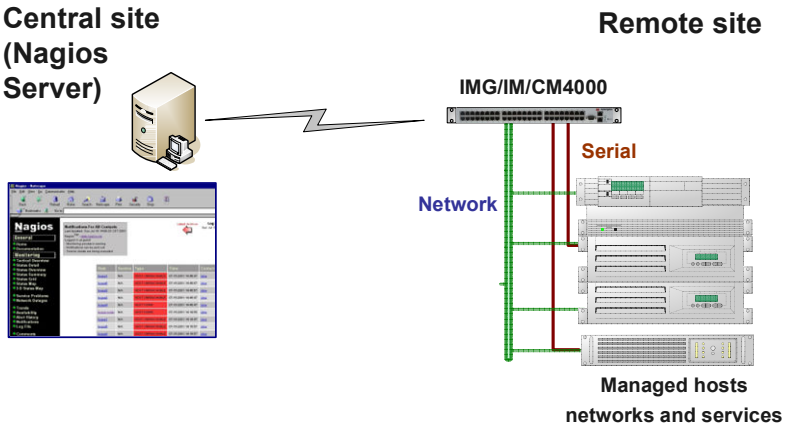
Chapter 10 Nagios Integration

Introduction

When deployed remotely to an upstream Nagios monitoring server the IMG/IM/CM4000 functions as a distributed monitoring server. The IMG/IM/CM4000 gateway embeds an NSCA (Nagios Service Checks Acceptor) client and NRPE (Nagios Remote Plugin Executor) server addons, so they can monitor attached serial devices and managed hosts and services, and remove the need for a dedicated slave Nagios server at the remote site.

The IMG/IM/CM4000 products all support basic distributed monitoring, whereas both IMG/IM4000 families also support extensive customizable distributed monitoring. The IMG/IM/CM4000 gateways can also be deployed locally to the Nagios monitoring host server to provide additional diagnostics and points of access to managed devices. This chapter describes:

- activating and configuring Nagios distributed monitoring using the IMG/IM/CM4000
- configuration of Nagios and plugin operation, and
- various scenarios where distributed monitoring can be of value



10.1 Nagios overview

Nagios provides central monitoring of the hosts and services in your distributed network. Nagios is an open source program and you can freely download the latest version at http://www.nagios.com/download. You can also freely download the IMG/IM/CM4000 firmware which supports Nagios (version 2.2.3 and later). Nagios forms the core of many leading commercial system management solutions such as GroundWork (http://www.groundworkopensource.com)

While Nagios takes some time to configure and install, it provides an outstanding network-monitoring system. With Nagios you can:

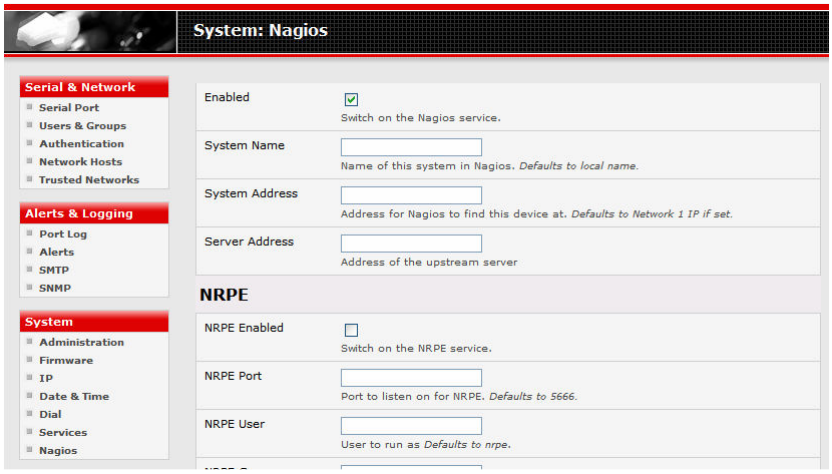
- display lists showing the status of each server, each network node and each service in real time
- use a wide range of freely available plugins to make detailed checks of specific services (e.g. don't just check a database is accepting network connections, check that it can actually validate requests and return real data)
- display warnings and send warning e-mails or pagers alerts when a service failure or degradation is detected
- assign contact groups who are responsible for specific services in specific time frames

10.2 Configuring Nagios

To activate the IMG/IM/CM4000Nagios distributed monitoring:

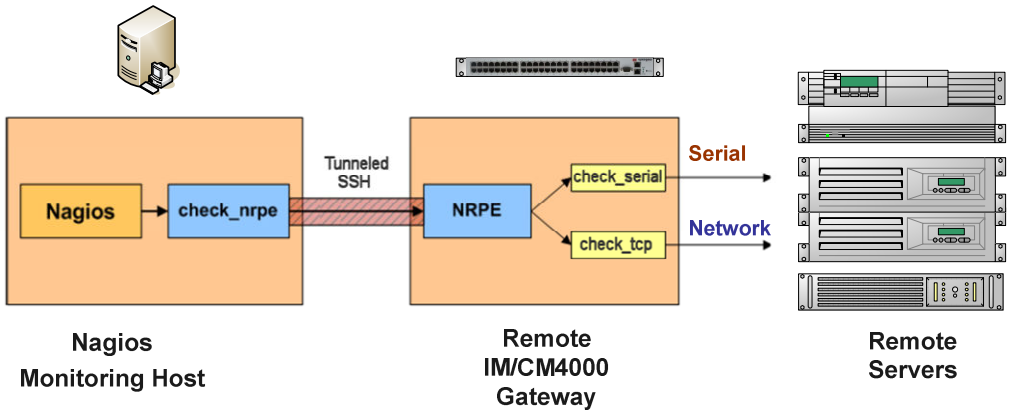
- Nagios integration must be enabled and a path established to the upstream Nagios server
- If the IMG/IM/CM4000 is to periodically report on Nagios monitored services, then the NSCA client embedded in the IMG/IM/CM4000 must be configured. The NSCA program enables scheduled check-ins with the remote Nagios server and is used to send passive check results across the network to the remote server
- If the Nagios server is to actively request status updates from the IMG/IM/CM4000, then the NRPE server embedded in the IMG/IM/CM4000 must be configured. The NRPE server is the Nagios daemon for executing plugins on remote hosts
- Each of the Serial Ports and each of the Hosts connected to the IMG/IM/CM4000 which are to be monitored must have Nagios enabled and any specific Nagios checks configured
- Lastly the upstream Nagios monitoring host must be configured

10.2.1 Enable Nagios on the IMG/IM/CM4000

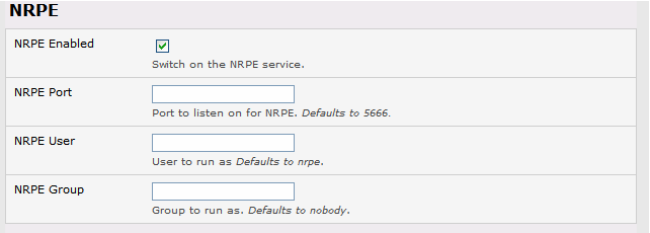


- On the IMG/IM/CM4000 Management Console select **System: Nagios** and **Enable** the Nagios service
- Enter the **Name** and **Address** details of the IMG/IM/CM4000 gateway and the IP **Address** of the upstream Nagios monitoring server

10.2.2 Enable NRPE monitoring



Enabling NRPE allows you to execute plugins (such as *check_tcp* and *check_ping*) on the remote IMG/IM/CM4000 gateway to monitor serial or network attached remote servers. This will offload CPU load from the upstream Nagios monitoring machine which is especially valuable if you are monitoring hundreds or thousands of hosts. To enable NRPE:

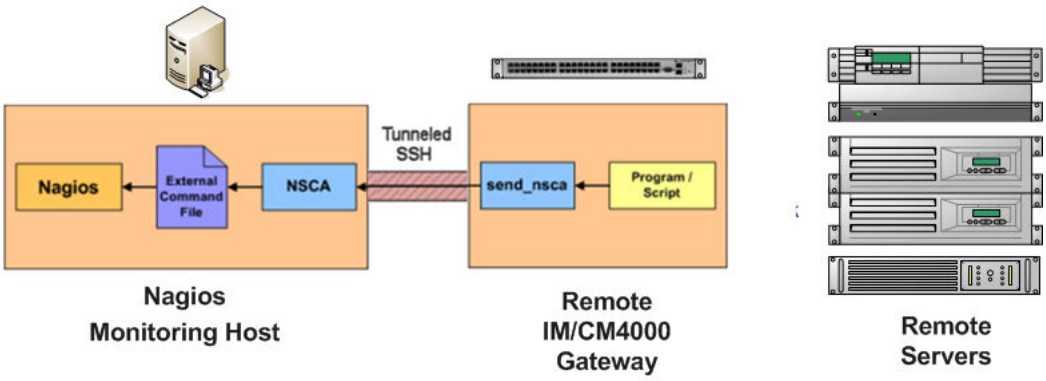


- Select **System: Nagios** and check **NRPE Enabled**

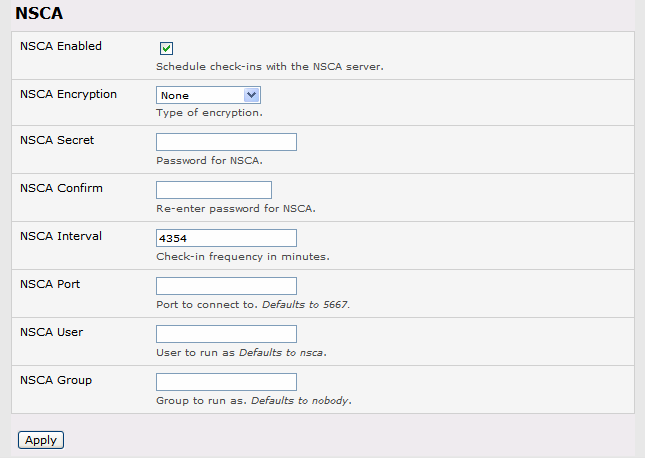
- Enter the details the user connection to the upstream Nagios monitoring server and again refer the sample Nagios configuration example below for details of configuring specific NRPE checks

By default the IMG/IM/CM4000 will accept a connection between the upstream Nagios monitoring server and the NRPE server with SSL encryption, without SSL, or tunneled through SSH. The security for the connection is configured at the Nagios server.

10.2.3 Enable NSCA monitoring



NSCA is the mechanism that allows you to send passive check results from the remote IMG/IM/CM4000 to the Nagios daemon running on the monitoring server. To enable NSCA:



- Select **System: Nagios** and check **NSCA Enabled**
- Select the **Encryption** to be used from the drop down menu, then enter a **Secret** password and specify a check **Interval**
- Refer the sample Nagios configuration section below for some examples of configuring specific NSCA checks

10.2.4 Configure selected Serial Ports for Nagios monitoring

The individual Serial Ports connected to the IMG/IM/CM4000 to be monitored must be configured for Nagios checks.

Refer *Chapter 4.4 – Network Host Configuration* for details on enabling Nagios monitoring for Hosts that are network connected to the IMG/IM/CM4000. To enable Nagios to monitor on a device connected to the IMG/IM/CM4000 serial port:

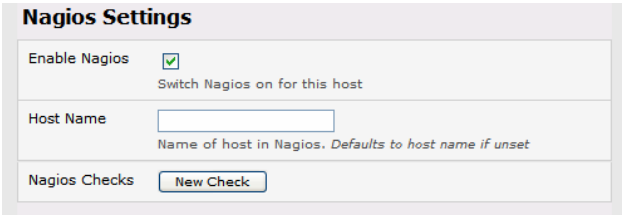
- Select **Serial&Network: Serial Port** and click **Edit** on the serial Port # to be monitored
- Select **Enable Nagios,** specify the name of the device on the upstream server and determine the check to be run on this port. **Serial Status** monitors the handshaking lines on the serial port and **Check Port** monitors the data logged for the serial port

.

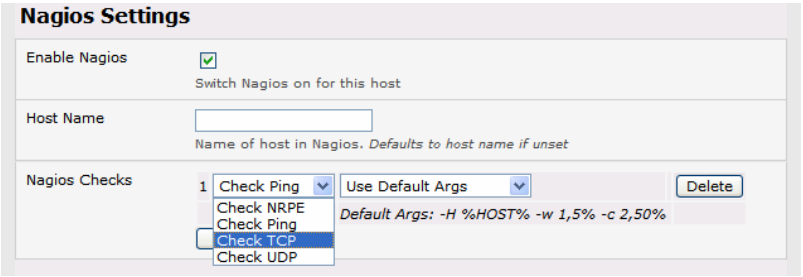
10.2.5 Configure selected Network Hosts for Nagios monitoring

The individual Network Hosts connected to the IMG/IM/CM4000 to be monitored must also be configured for Nagios checks:

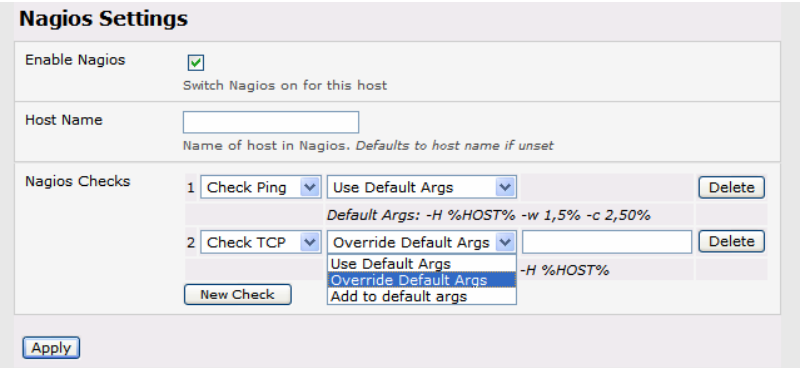
- Select **Serial&Network: Network Port** and click **Edit** on the Network Host to be monitored



- Select **Enable Nagios,** specify the name of the device on the upstream server and select **New Check** to add a specific check which will be run on this host



- You can then customize the selected **Nagios Checks** to use custom arguments
- Click **Apply**



10.2.6 Configure the upstream Nagios monitoring host

Refer to the Nagios documentation for configuring the upstream server:

- http://nagios.sourceforge.net/docs/2_0/distributed.html steps through what you need to do to configure NSCA on the upstream server (under *central server config*)
- *NRPE Documentation* has recently been added which steps through configuring NRPE on the upstream server http://nagios.sourceforge.net/docs/nrpe/NRPE.pdf

At this stage, Nagios at the upstream monitoring server has been configured, and individual serial port and network host connections on the IMG/IM/CM4000 configured for Nagios monitoring. If NSCA is enabled, each selected check will be executed once over the period of the check interval. If NRPE is enabled, then the upstream server will be able to request status updates under it's own scheduling.

10.3 Advanced Configuration

10.3.1 Sample Nagios configuration

An example configuration for Nagios is listed below. It shows how to set up a remote IMG/IM/CM4000 gateway to monitor a single host, with both network and serial connections. For each check it has two configurations, one each for NRPE and NSCA.

In practice, these would be combined into a single check which used NSCA as a primary method, falling back to NRPE if a check was late (for details see the Nagios documentation on *Freshness* http://nagios.sourceforge.net/docs/1_0/freshness.html).

```
; Host definitions
;
; Opengear IMG/IM/CM4000 gateway
define host{
        use             generic-host
        host_name           opengear
        alias           IMG/IM/CM4000 Gateway
        address           192.168.254.147
        }

; Managed Host
define host{
        use             generic-host
        host_name           server
        alias           server
        address           192.168.254.227
        }

; NRPE daemon on gateway
define command {
        command_name      check_nrpe_daemon
        command_line$USER1$/check_nrpe -H 192.168.254.147 -p 5666
        }

define service {
        service_description   NRPE Daemon
        host_name             opengear
        use                   generic-service
        check_command               check_nrpe_daemon
        }


; Serial Status
define command {
        command_name      check_serial_status
        command_line$USER1$/check_nrpe -H 192.168.254.147 -p 5666 -c
check_serial_$HOSTNAME$
        }

define service {
        service_description   Serial Status
        host_name             server
        use                   generic-service
        check_command               check_serial_status
        }
```

```
define service {
        service_description     serial-signals-server
        host_name               server
        use                     generic-service
        check_command                   check_serial_status
        active_checks_enabled           0
        passive_checks_enabled          1
        }

define servicedependency{
        name                            opengear_nrpe_daemon_dep
        host_name                       opengear
        dependent_host_name                     server
        dependent_service_description           Serial Status
        service_description             NRPE Daemon
        execution_failure_criteria      w,u,c
        }


; Port Log
define command{
        command_name    check_port_log
        command_line    $USER1$/check_nrpe -H 192.168.254.147 -p 5666 -c
port_log_$HOSTNAME$
      }

define service {
        service_description     Port Log
        host_name               server
        use                     generic-service
        check_command                   check_port_log
        }

define service {
        service_description     port-log-server
        host_name               server
        use                     generic-service
        check_command                   check_port_log
        active_checks_enabled           0
        passive_checks_enabled          1
        }

define servicedependency{
        name                            opengear_nrpe_daemon_dep
        host_name                       opengear
        dependent_host_name                     server
        dependent_service_description           Port Log
        service_description             NRPE Daemon
        execution_failure_criteria      w,u,c
        }
```

```
; Ping
define command{
        command_name    check_ping_via_opengear
        command_line    $USER1$/check_nrpe -H 192.168.254.147 -p 5666 -c
host_ping_$HOSTNAME$
      }

define service {
        service_description     Host Ping
        host_name               server
        use                     generic-service
        check_command                   check_ping_via_opengear
        }

define service {
        service_description     host-ping-server
        host_name               server
        use                     generic-service
        check_command                   check_ping_via_opengear
        active_checks_enabled       0
        passive_checks_enabled      1
        }

define servicedependency{
        name                            opengear_nrpe_daemon_dep
        host_name                       opengear
        dependent_host_name                     server
        dependent_service_description       Host Ping
        service_description             NRPE Daemon
        execution_failure_criteria      w,u,c
        }


; SSH Port
define command{
      command_name    check_conn_via_opengear
      command_line    $USER1$/check_nrpe -H 192.168.254.147 -p 5666 -c
host_$HOSTNAME$_$ARG1$_$ARG2$
      }

define service {
        service_description     SSH Port
        host_name               server
        use                     generic-service
        check_command                   check_conn_via_opengear!tcp!22
        }

define service {
        service_description     host-port-tcp-22-server
```

```
                        ; host-port-<protocol>-<port>-<host>
        host_name       server
        use             generic-service
        check_command           check_conn_via_opengear!tcp!22
        active_checks_enabled   0
        passive_checks_enabled  1
        }

define servicedependency{
        name                            opengear_nrpe_daemon_dep
        host_name                       opengear
        dependent_host_name                     server
        dependent_service_description   SSH Port
        service_description             NRPE Daemon
        execution_failure_criteria      w,u,c
        }
```

10.3.2 Basic Nagios plugins

Plugins are compiled executables or scripts that can be scheduled to be run on the IMG/IM/CM4000 to check the status of a connected host or service. This status is then communicated to the upstream Nagios server which uses the results to monitor the current status of the distributed network.

Each IMG/IM/CM4000 is preconfigured with a selection of the checks that are part of the Nagios plugins package:

check_tcp and *check_udp* are used to check open ports on network hosts

check_ping is used to check network host availability

check_nrpe is used to execute arbitrary plugins in other devices

Each IMG/IM/CM4000 is preconfigured with two checks that are specific to Opengear:

check_serial_signals is used to monitor the handshaking lines on the serial ports

check_port_log is used to monitor the data logged for a serial port.

10.3.3 Additional plugins (IMG4xxx and IM42xx only)

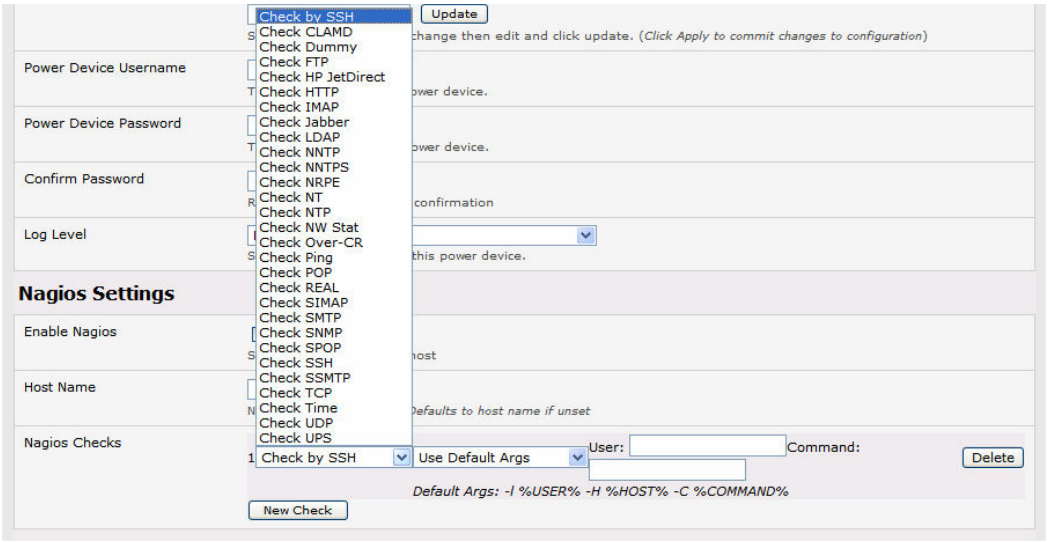
Additional Nagios plugins (listed below) are available for all the IMG/IM4000 products:

check_apt	*check_http*	*check_nt*	*check_snmp*
check_by_ssh	*check_imap*	*check_ntp*	*check_spop*
check_clamd	*check_jabber*	*check_nwstat*	*check_ssh*
check_dig	*check_ldap*	*check_overcr*	*check_ssmtp*
check_dns	*check_load*	*check_ping*	*check_swap*
check_dummy	*check_mrtg*	*check_pop*	*check_tcp*
check_fping	*check_mrtgtraf*	*check_procs*	*check_time*
check_ftp	*check_nagios*	*check_real*	*check_udp*
check_game	*check_nntp*	*check_simap*	*check_ups*
check_hpjd	*check_nntps*	*check_smtp*	*check_users*

These plugins from the Nagios plugins package can be downloaded from ftp.opengear.com.

There also are *bash* scripts which can be downloaded and run (primarily *check_log.sh).*

- To configure additional checks the downloaded plugin program must be saved in the tftp *addins* directory on the USB flash and the downloaded text plugin file saved in */etc/config*
- To enable these new additional checks you select **Serial&Network: Network Port**, then **Edit** the Network Host to be monitored, and select **New Checks**. The additional check option will have been included in the updated **Nagios Checks** list, and you can again customize the arguments



If you need other plugins to be loaded into the IMG/IM4000 firmware:

- If the plugin in a Perl script, it must be rewritten as the IMG/IM/CM4000 does not support Perl at this point. However, if you do require Perl support, please make a feature request to support@opengear.com
- Individual compiled programs may be generated using *gcc* for ARM. Again contact support@opengear.com for details

10.3.4 Number of supported devices

Ultimately the number of devices that can be supported by any particular IMG/IM/CM4000 is a function of the number of checks being made, and how often they are performed. Access method will also play a part.

The table below shows the performance of three of the IMG/IM/CM4000 models (1/2 port, 8 port and 16/48 port) tabulating:

Time	No encryption	3DES	SSH tunnel
NSCA for single check	~ ½ second	~ ½ second	~ ½ second
NSCA for 100 sequential checks	100 seconds	100 seconds	100 seconds
NSCA for 10 sequential checks, batched upload	1 ½ seconds	2 seconds	1 second
NSCA for 100 sequential checks, batched upload	7 seconds	11 seconds	6 seconds

	No encryption	SSL	no encryption - tunneled over existing SSH session
NRPE time to service 1 check	1/10th second	1/3rd second	1/8th second
NRPE time to service 10 simultaneous checks	1 second	3 seconds	1 ¼ seconds
Maximum number of simultaneous checks before timeouts	30	20 (1,2 and 8) or 25 (16 and 48 port)	25 (1,2 and 8 port), 35 (16 and 48 port)

The results were from running tests 5 times in succession with no timeouts on any runs. However there are a number of ways to increase the number of checks you can do:

Usually when using NRPE checks, an individual request will need to set up and tear down an SSL connection. This overhead can be avoided by setting up an SSH session to the IMG/IM/CM4000 and tunneling the NRPE port. This allows the NRPE daemon to be run securely without SSL encryption, as SSH will take care of the security.

When the IMG/IM/CM4000 submits NSCA results it staggers them over a certain time period (e.g. 20 checks over 10 minutes will result in two check results every minute). Staggering the results like this means that in the event of a power failure or other incident that causes multiple problems, the individual freshness checks will be staggered too.

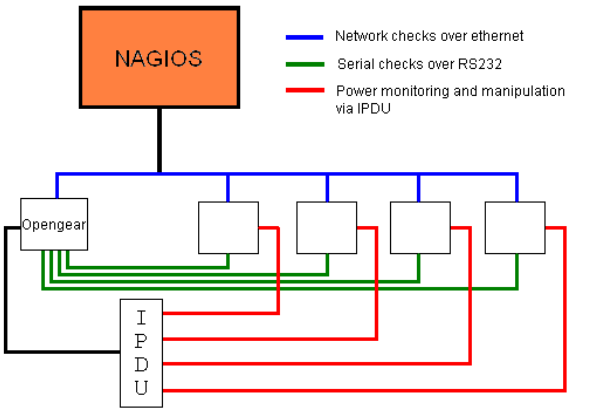
NSCA checks are also batched. So in the previous example the two checks per minute will be sent through in a single transaction.

10.4 Usage scenarios

Below are a number of distributed monitoring Nagios scenarios:

10.4.1 Local office

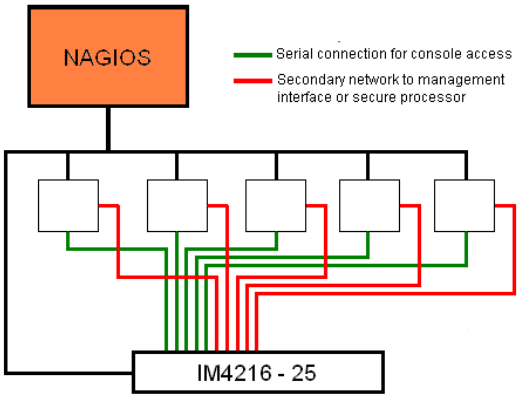
In this scenario, the IMG/IM/CM4000 is set up to monitor the console of each managed device. It can be configured to make a number of checks, either actively at the Nagios server's request, or passively at preset intervals, and submit the results to the Nagios server in a batch. The IMG/IM/CM4000 may be augmented at the local office site by one or more Intelligent Power Distribution Units (IPDUs) to remotely control the power supply to the managed devices.



]

10.4.2 Local office using IM4216-25

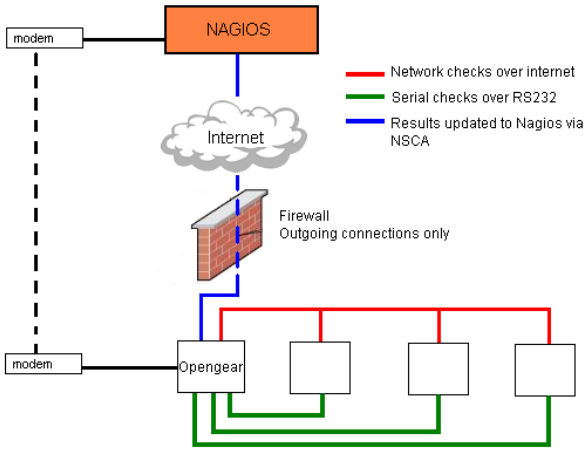
In this scenario the IM4216-25 is used to provide the management network in the office. The IM4216-25 has sixteen serial ports for monitoring the consoles of managed devices, or to interface to an IPDU. It also has a total of 25 Ethernet ports, of which 24 are designed to be connected to management network ports or service processors. The IM4216-25 provides secured, audited, and easily managed access to the management network. Further, each of the Ethernet ports is isolated from the others, meaning each managed device is unable to interfere with other managed devices, including sniffing data.



A similar solution is to use an IM4216-2 or IM4248-2 and connect its second Ethernet port up to an external switch to provide the management network connections:

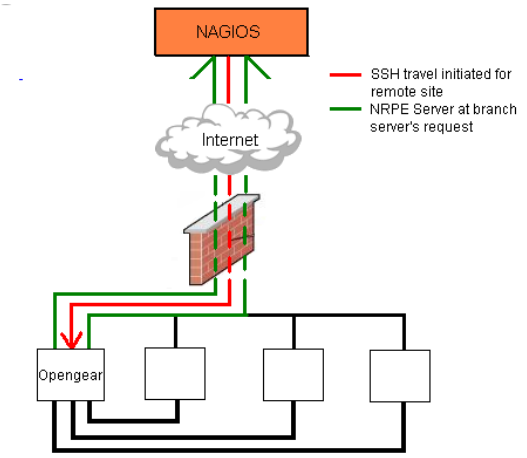
10.4.3 Remote site

In this scenario the IMG/IM/CM4000 NRPE server or NSCA client can be configured to make active checks of configured services and upload to the Nagios server waiting passively. It can also be configured to service NRPE commands to perform checks on demand. In this situation, the IMG/IM/CM4000 will perform checks based on both serial and network access.



10.4.4 Remote site with restrictive firewall

In this scenario the role of the IMG/IM/CM4000 will vary. One aspect may be to upload check results through NSCA. Another may be to provide an SSH tunnel to allow the Nagios server to run NRPE commands.



10.4.5 Remote site with no network access

In this scenario the IMG/IM/CM4000 allows dial-in access for the Nagios server. Periodically, the Nagios server will establish a connection to the IMG/IM/CM4000 and execute any NRPE commands, before dropping the connection.

Chapter 11 System Management

Introduction

This chapter describes how the Administrator can perform a range of general IMG/IM/CM4000 system administration and configuration tasks such as:

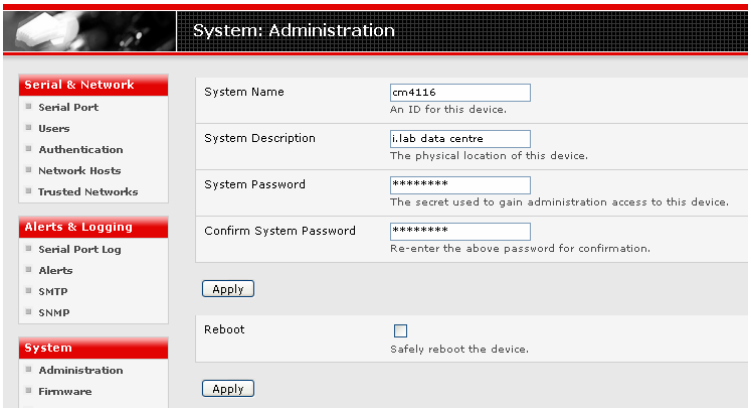
- Applying *Soft* and *Hard* Resets to the gateway
- Reflashing the Firmware
- Configuring the Date, Time and NTP

System administration and configuration tasks are covered elsewhere include:

- Resetting the System Password and entering a new System Name and Description for the IMG/IM/CM4000 gateway (*Chapter 3.2*)
- Setting the gateway's System IP Address (*Chapter 3. 3)*
- Setting the permitted Services by which to access the gateway (*Chapter 3.4*)
- Setting up OoB Dial-in (*Chapter 5*)

11.1 System Administration and Reset

The Administrator can reboot or reset the gateway to default settings.



A *soft* reset is affected by:

- Selecting **Reboot** in the **System: Administration** menu and clicking **Apply**

The IMG/IM/CM4000 reboots with all settings (*e.g.* the assigned network IP address) preserved. However this *soft* reset does disconnect all Users and ends any SSH sessions that had been established.

A *soft* reset will also be affected when you switch OFF power from the IMG/IM/CM4000, and then switch the power back ON. However if you cycle the power and the unit is writing to flash you could corrupt or lose data, so the software reboot is the safer option.

A *hard* erase (*hard reset*) is effected by:

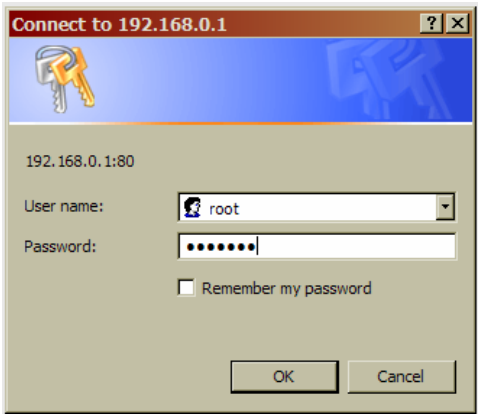
- Pushing the *Erase* button on the rear panel **twice**. A ball point pen or bent paper clip is a suitable tool for performing this procedure. Do not use a graphite pencil. Depress the button gently **twice** (within a 5 second period) while the unit is powered ON.

This will reset the IMG/IM/CM4000 back to its factory default settings and clear the IMG/IM/CM4000's stored configuration information.

The *hard* erase will clear all custom settings and return the unit back to factory default settings (*i.e.* the IP address will be reset to 192.168.0.1).

You will be prompted to log in and must enter the default administration username and administration password:

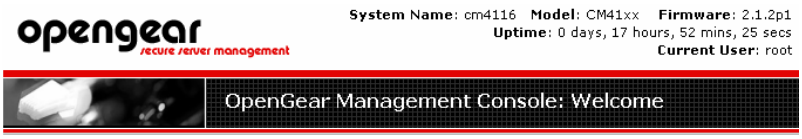
Username: **root**
Password: **default**



11.2 Upgrade Firmware

Before upgrading you should ascertain if you are already running the most current firmware in your gateway. Your IMG/IM/CM4000 will not allow you to upgrade to the same or an earlier version.

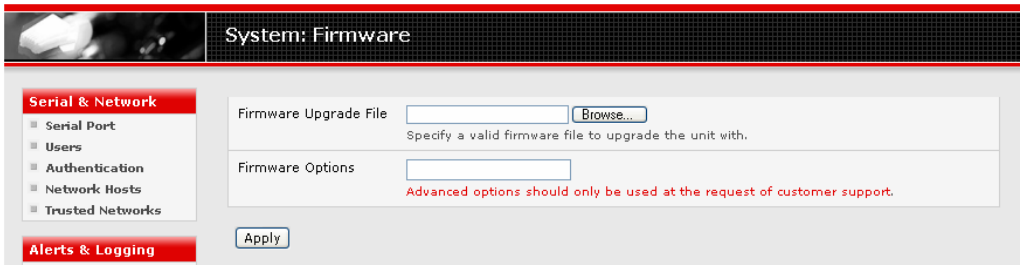
- The **Firmware** version is displayed in the header of each page



- Or select **Status: Support Report** and note the **Firmware Version**

- To upgrade, you first must download the latest firmware image from ftp://ftp.opengear.com :
  - For CM4001 download the *cm4002.flash* file
  - For CM4008 download the *cm4008.flash* file and
  - For both CM4116 and CM4148 download *cm41xx.flash*
  - For IM4216-2, IM4216-25 and IM4148-2 download *im42xx.flash*

- *S*ave this downloaded firmware image file on to a system on the same subnet as the IMG/IM/CM4000

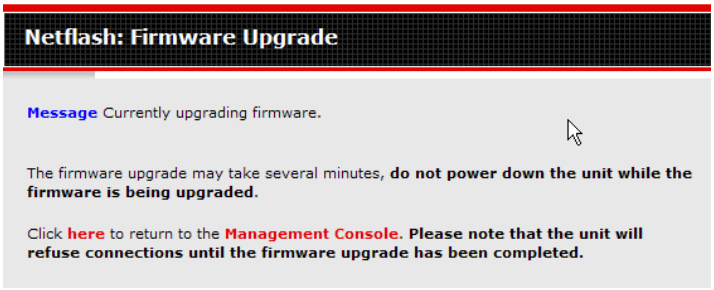


- Also download and read the *release_notes.txt* for the latest information

- To then up-load the firmware image file to your IMG/IM/CM4000, select **System: Firmware**

- Specify the address and name of the downloaded Firmware Upgrade File, or **Browse** the local subnet and locate the downloaded file

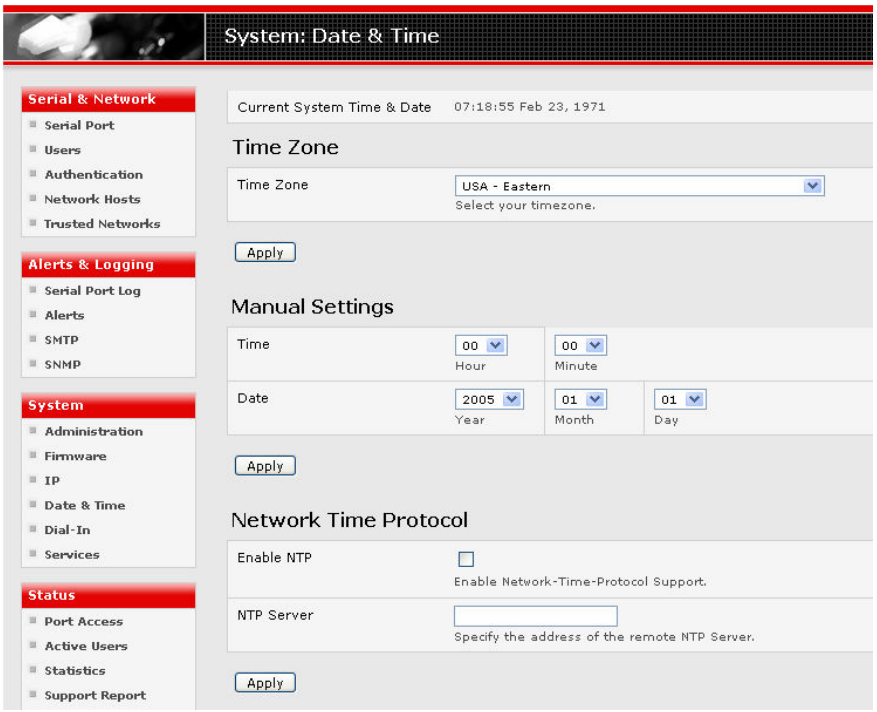
- Click **Apply** and the IMG/IM/CM4000 appliance will undertake a soft reboot and commence upgrading the firmware. This process will take several minutes



- After the firmware upgrade has completed, click **here** to return to the Management Console. Your IMG/IM/CM4000 will have retained all its pre-upgrade configuration information

11.3 Configure Date and Time

It is recommended that you set the local Date and Time in the IMG/IM/CM4000 as soon as it is configured. Features like Syslog and NFS logging, use the system time for time-stamping log entries, while certificate generation depends on a correct *Timestamp* to check the validity period of the certificate.



- Select the **System: Date & Time** menu option
- Manually set the **Year**, **Month**, **Day**, **Hour** and **Minute** using the **Date** and **Time** selection boxes, then click **Apply**

The gateway can synchronize its system time with a remote time server using the Network Time Protocol (NTP). Configuring the NTP time server ensures that the IMG/IM/CM4000 clock will be accurate soon after the Internet connection is established. Also if NTP is not used, the system clock will be reset randomly every time the IMG/IM/CM4000 is powered up. To set the system time using NTP:

- Select the **Enable NTP** checkbox on the **Network Time Protocol** page
- Enter the IP address of the remote **NTP Server** and click **Apply**

You must now also specify your local time zone so the system clock can show local time (and not UTP):

- Set your appropriate region/locality in the **Time Zone** selection box and click **Apply**

Chapter 12 Status Reports

Introduction

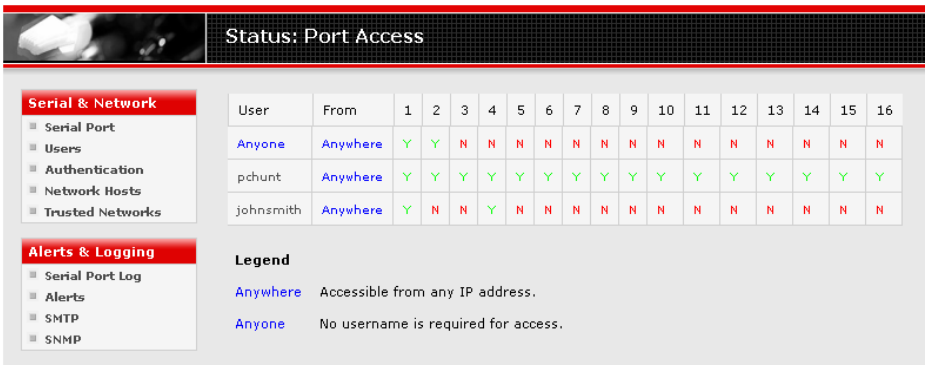
This chapter describes the selection of status reports that are available for review:

- Port Access and Active Users
- Statistics
- Support Reports
- Syslog

12.1 Port Access and Active Users

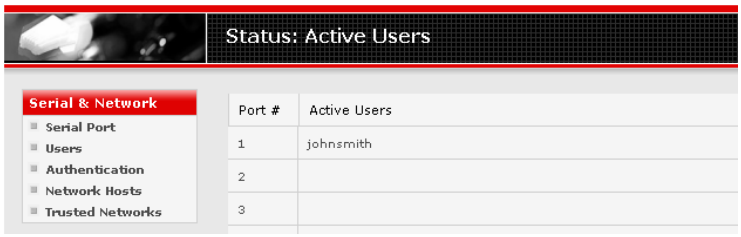
The Administrator can see which Users have access privileges with which ports:

➢ Select the **Status: Port Access**



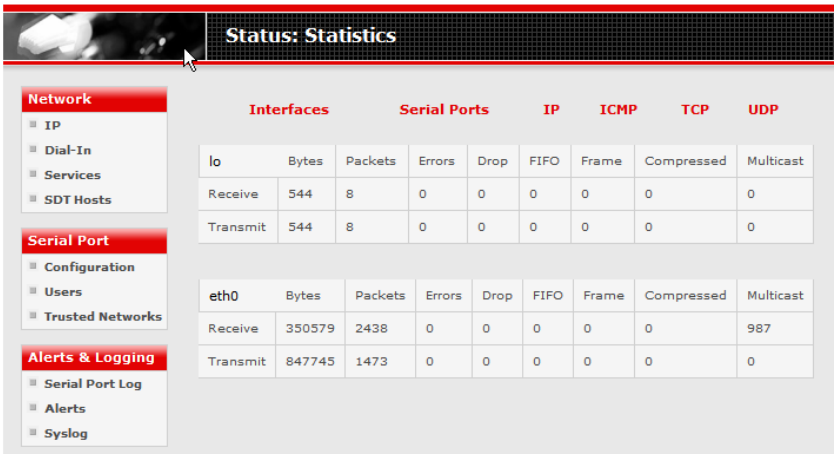
The Administrator can also see the current status as to Users who have active sessions on those ports:

➢ Select the **Status: Active Users**



12.2 Statistics

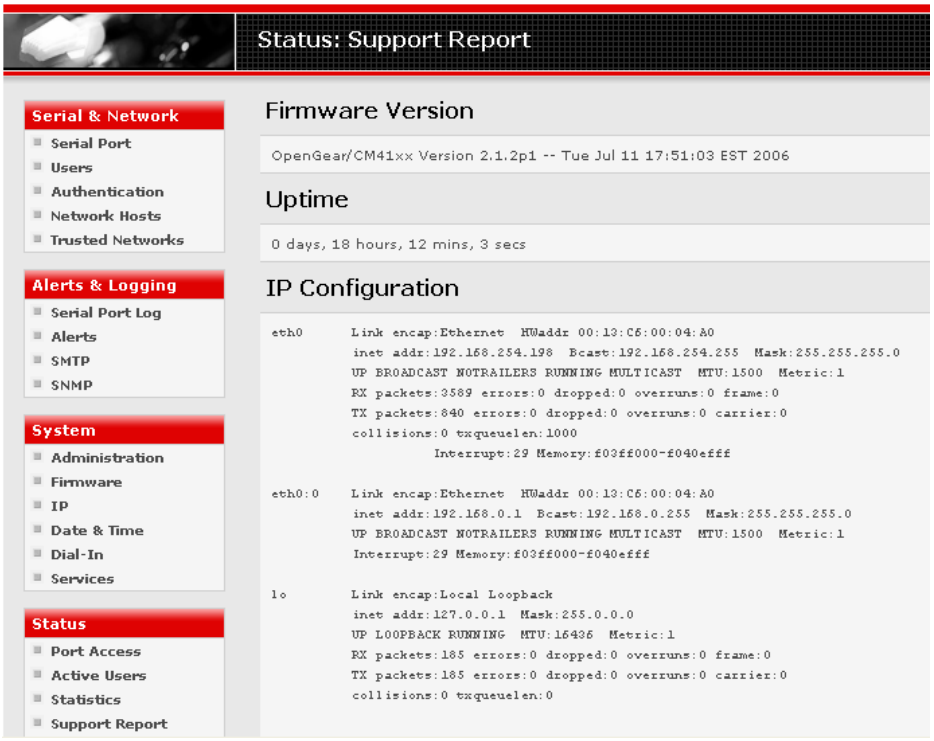
The Statistics report provides a snapshot of the data traffic and other activities and operations of your gateway.



12.3 Support Reports

The Support Report provides useful status information that will assist the Opengear technical support team to solve any problems you may experience with your IMG/IM/CM4000.

If you do experience a problem and have to contact support, ensure you include the Support Report with your email support request. The Support Report should be generated when the issue is occurring, and attached in plain text format.



- Select the **Status: Support Report** menu option and you will be presented with a snapshot of your gateway's status
- Save the file as a text file and attach it to your support email

12.4 Syslog

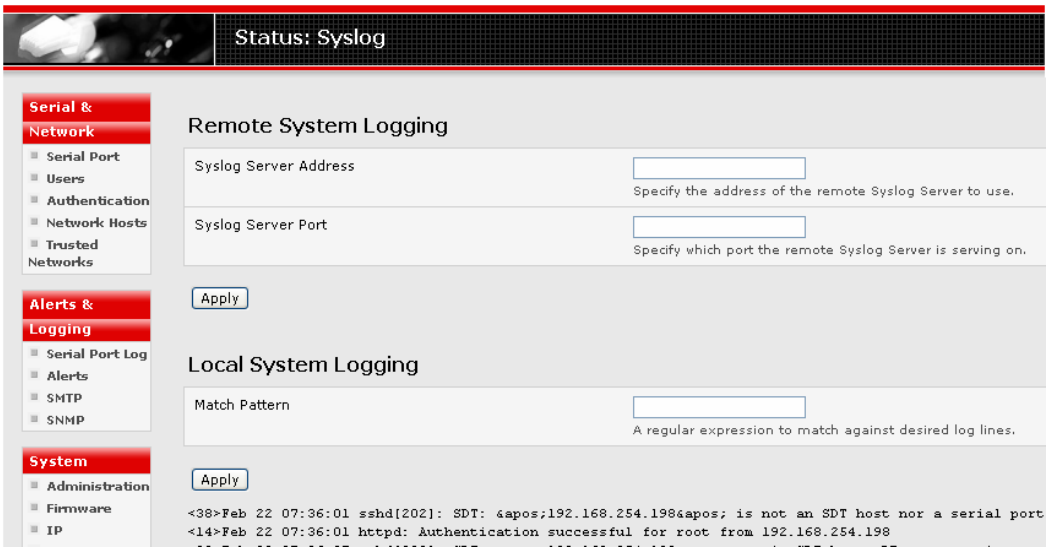
The Linux System Logger maintains a record of all system messages and errors:

- Select **Status: Syslog**

Remote System Logging

The syslog record can be redirected to a remote Syslog Server:

- Enter the remote Syslog Server address and port details and click **Apply**



Local System Logging

To view the local Syslog file:

- Select **Alerts & Logging: Syslog**

To make it easier to find information in the local Syslog file, a pattern matching filter tool is provided.

- Specify the **Match Pattern** that is to be searched for (*e.g.* the search for *Mount* is shown below) and click **Apply.** The Syslog will then be represented with only those entries that actually include the specified pattern

Chapter 13 Management

Introduction

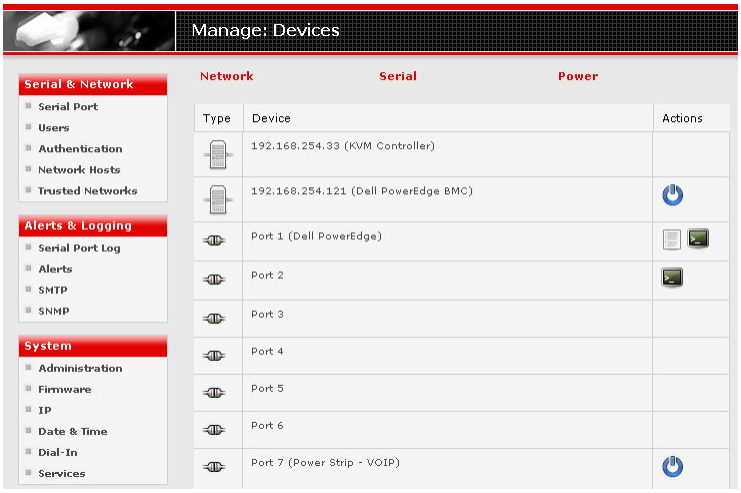
The IMG/IM/CM4000 has a number of Management reports and tools that can be accessed by both Administrators and Users:

- Access and control configured devices
- View serial port logs and host logs
- Use the in-built java terminal to access serially attached consoles
- Power control

13.1 Device Management

To display all the connected Serial devices, Network Hosts and Power devices:

➢ Select **Manage: Devices.** By then selecting the **Serial/ Network/ Power** item, the display will be reduced to such devices only

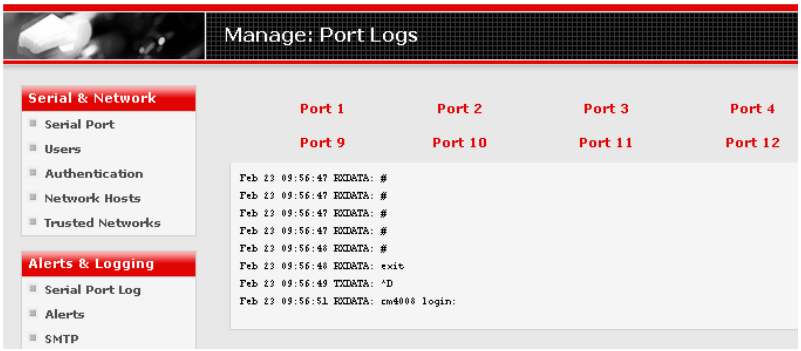


The user can take a range of actions on each of these Serial/Network/Power devices by selecting the **Action** icon or the related Manage menu item. Selecting the Manager Power icon or the **Manage: Power** menu for is covered in *Chapter 8.*

13.2 Port Log Management

Administrator and Users can view logs of data transfers to connected devices.

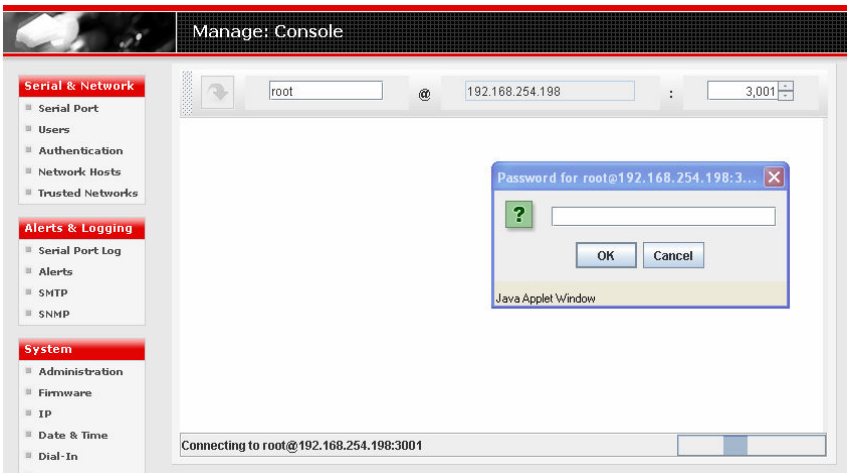
- Select **Manage: Port Logs** and the serial Port # to be displayed:



- To display Host logs select **Manage: Host Logs** and the Host # to be displayed

13.3 Serial Port Terminal Management

Administrator and Users can communicate directly with devices attached to the IMG/IM/CM4000 serial ports using the in-built terminal. This virtual terminal access is provided by running *jcterm* (a java vt100 terminal client) from the browser and connecting to the serial port using SSH.



- Select **Manage: Terminal** and the virtual terminal will be displayed with the gateway's TCP address (e.g. *192.168.254.198*), the Username (e.g. *root*) and the TCP Port address for the serial port to be accessed. By default *3001* is selected (i.e. Port 1). To access Port 4 for example, this must be changed to *3004*

- Enter the **Password** for the Username

Chapter 14 Basic Configuration - Linux Commands

Introduction

For those who prefer to configure their IMG/IM/CM4000 at the Linux command line level (rather than use a browser and the Management Console), this chapter describes getting command line access and using the ***config*** tool to manage the system and configure the ports *etc.* from the command line:

- Administration Configuration (System Settings and Authentication Configuration)
- Date and Time Configuration (Manually Change Clock Settings and Network Time Protocol Time Zone)
- Network Configuration (Static and DHCP IP Configuration, Dial-in Configuration and Services Configuration)
- Serial Port Configuration (Serial Port Settings, Supported Protocol Configuration, Users and Trusted Networks)
- Event Logging Configuration (Remote Serial Port Log Storage and Alert Configuration)

The *config* documentation in this chapter walks thru basic configuration (in line with what can be done with the Management Console). For advanced and custom configurations using other standard commands refer to the next chapter, *Advanced Configuration.*

The IMG/IM/CM4000 runs a standard Linux kernel so it is also possible to configure the gateway using other standard Linux and Busybox commands and applications (*ifconfig, gettyd, stty etc.*) However doing this will not guarantee these changes are permanent.

WARNING

This chapter is not intended to teach you Linux. We assume you already have a certain level of understanding before you execute Linux kernel level commands.

14.1 The Linux Command line

- Power up the IMG/IM/CM4000 and connect the “terminal” device:
  - If you are connecting using the serial line, plug a serial cable between the IMG/IM/CM4000 local DB-9 port and terminal device. Configure the serial connection of the “terminal” device/program you are using to 115200bps, 8 data bits, no parity and one stop bit. If you are using a program running on a Windows PC as the terminal device, then the cable is made up from a Cat5 UTP (#440016) cable and two DB-9 to RJ-45 adapters (#319000 and #319001)
  - If you are connecting over the LAN then you will need to interconnect the Ethernet ports and direct your terminal emulator program to the IP address of the IMG/IM/CM4000 (192.168.0.1 by default)
- Log on to the IMG/IM/CM4000 by pressing ‘return’ a few times. The IMG/IM/CM4000 will request a username and password. Enter the username *root* and the password *default*. You should now see the command line prompt which is a hash (#)

The config Tool

Syntax

config [-ahv] [-d id] [-g id] [-p path] [-r configurator] [-s id=value]

Description

The config tool allows manipulation and querying of the system configuration from the command line. Using config, the new configuration can be activated by running the relevant *configurator* which performs the action necessary to make the configuration changes live.

Configuration elements which can be changed are specified by a unique '.' separated name. For example the configuration file version is identified as '*config.version*'.

The config tool is designed to perform multiple actions from one command if need be, so if necessary options can be chained together.

Options

-a **–run-all** Run all registered configurators. This performs every configuration synchronization action pushing all changes to the live system

-h –help Display a brief usage message.

-v –verbose Log extra debug information

-d –del=id Remove the given configuration element specified by a '.' separated identifier.

-g –get=id Display the value of a configuration element.

-p –path=file Specify an alternate configuration file to use. The default file is located at */etc/config/config.xml*

-r –run=configurator Run the specified registered configurator. Registered configurators are alerts, auth, dialin, eventlog, ipconfig, power, serialconfig, services, systemsettings, time and users.

-s --set=id=value Change the value of configuration element specified by a '.' separated identifier.

14.2 Administration Configuration

System Settings

To change system settings to the following values:

System Name	og.mydomain.com
System Password (root account)	secret
System SMTP Server	192.168.0.124
System SMTP Sender	og@mydomain.com

```
The following commands must be issued:
# /bin/config --set=config.system.name=og.mydomain.com
# /bin/config --set=config.system.password=secret
# /bin/config --set=config.system.smtp.server=192.168.0.124
# /bin/config --set=config.system.smtp.sender=og@mydomain.com
The following command will synchronize the live system with the
new configuration.
# /bin/config --run=systemsettings
```

Authentication Configuration

You can configure the system remote authentication with the following settings:

Remote Authentication Method	LDAP
Server IP Address	192.168.0.32
Server Password	Secret
LDAP Base Node	Some base node

By issuing the following commands:

```
# /bin/config --set=config.auth.type=LDAP
# /bin/config --set=config.auth.server=192.168.0.32
# /bin/config --set=config.auth.password=Secret
# /bin/config --set="config.auth.ldap.basenode=some base node"
```

The following command will synchronize the live system with the new configuration.

```
# /bin/config --run=auth
```

14.3 Date and Time Configuration

Manually Change Clock Settings

To change the running system time you need to issue the following commands:

```
#  date 092216452005.05       Format is MMDDhhmm[[CC]YY][.ss]
```

Then the following command will save this new system time to the hardware clock:

```
# /bin/hwclock -systohc
```

Alternately to change the hardware clock time you need to issue the following commands:

```
# /bin/hwclock --set --date=092216452005.05
Where the format is MMDDhhmm[[CC]YY][.ss]
```

Then the following command will save this new hardware clock time as the system time:

```
# /bin/hwclock -hctosys
```

Network Time Protocol

To enable NTP using a server at pool.ntp.org issue the following commands:

```
# /bin/config --set=config.ntp.enabled=on
# /bin/config --set=config.ntp.server=pool.ntp.org
```

The following command will synchronize the live system with the new configuration.

```
# /bin/config --run=time
```

Time Zone

To change the system time zone USA eastern standard time you need to issue the following commands:

```
# /bin/config --set=config.system.timezone=US/Eastern
```

The following command will synchronize the live system with the new configuration.

```
# /bin/config --run=time
```

14.4 Network Configuration

IP Configuration

DHCP

To enable a DHCP client on the LAN interface (eth0) from the gateway command line:

```
# /bin/config --set=config.interfaces.eth0.mode=dhcp
```

The following command will synchronize the live system with the new configuration.

```
# /bin/config --run=ipconfig
```

Note: “/bin/config” commands can be combined into one command for convenience.

Please note that supported interface modes are 'dhcp' and 'static'.

Static

To set static configuration on the LAN interface with the following attributes:

IP Address:	192.168.1.100
Network Mask:	255.255.255.0
Default Gateway:	192.168.1.1
Primary DNS:	192.168.1.254

IP Address:	192.168.1.100
Secondary DNS:	10.1.0.254

You would need to issue the following commands from the command line:

```
# /bin/config --set=config.interfaces.eth0.mode=static
# /bin/config --set=config.interfaces.eth0.address=192.168.1.100
# /bin/config --set=config.interfaces.eth0.netmask=255.255.255.0
# /bin/config --set=config.interfaces.eth0.gateway=192.168.1.1
# /bin/config --set=config.interfaces.eth0.dns1=192.168.1.254
# /bin/config --set=config.interfaces.eth0.dns2=10.1.0.254
```

The following command will synchronize the live system with the new configuration.

```
# /bin/config --run=ipconfig
```

Dial-in Configuration

To enable dial-in access on the DB9 serial port from the command line with the following attributes:

Local IP Address	172.24.1.1
Remote IP Address	172.24.1.2
Authentication Type: Serial Port Baud Rate:	MSCHAPv2 115200
Serial Port Flow Control: Custom Modem Initialization:	Hardware ATQ0V1H0

You would need to issue the following commands from the command line to set system configuration:

```
# /bin/config --set=config.console.ppp.localip=172.24.1.1
# /bin/config --set=config.console.ppp.remoteip=172.24.1.2
# /bin/config --set=config.console.ppp.auth=MSCHAPv2
# /bin/config --set=config.console.ppp.enabled=on
# /bin/config --set=config.console.speed=115200
# /bin/config --set=config.console.flow=Hardware
# /bin/config --set=config.console.initstring=ATQ0V1H0
```

The following command will synchronize the live system with the new configuration.

```
# /bin/config --run=dialin
```

Please note that supported authentication types are 'None', 'PAP', 'CHAP' and 'MSCHAPv2'.

Supported serial port baud-rates are '9600', '19200', '38400', '57600', '115200', and '230400'.

Supported parity values are 'None', 'Odd', 'Even', 'Mark' and 'Space'.

Supported data-bits values are '8', '7', '6' and '5'.

Supported stop-bits values are '1', '1.5' and '2'.

Supported flow-control values are 'Hardware', 'Software' and 'None'.

If you do not wish to use out-of-band dial-in access please note that the procedure for enabling start-up messages on the console port is covered in *Chapter 15 - Accessing the Console Port.*

Services Configuration

You can manually enable or disable network servers from the command line. For example if you wanted to guarantee the following server configuration:

HTTP Server	Enabled
HTTPS Server	Disabled
Telnet Server	Disabled
SSH Server	Enabled
SNMP Server	Disabled
Ping Replies (Respond to ICMP echo requests)	Disabled

You would need to issue the following commands from the command line to set system configuration:

```
# /bin/config --set=config.services.http.enabled=on
# /bin/config --del=config.services.https.enabled
# /bin/config --del=config.services.telnet.enabled
# /bin/config --set=config.services.ssh.enabled=on
# /bin/config --del=config.services.snmp.enabled
# /bin/config --del=config.services.pingreply.enabled
```

The following command will synchronize the live system with the new configuration.

```
# /bin/config --run=services
```

Note: “/bin/config” commands can be combined into one command for convenience.

14.5 Serial Port Configuration

Serial Port Settings

To setup serial port 5 to use the following properties:

Baud Rate	115200
Parity	None
Data Bits	8
Stop Bits	1
Flow Control	Software

You would need to issue the following commands from the command line to set the port configuration:

```
# /bin/config --set=config.ports.port5.speed=115200
# /bin/config --set=config.ports.port5.parity=None
# /bin/config --set=config.ports.port5.charsize=8
# /bin/config --set=config.ports.port5.stop=1
# /bin/config --set=config.ports.port5.flow=Software
```

The following command will synchronize the live system with the new configuration.

```
# /bin/config --run=serialconfig
```

Note that supported serial port baud-rates are ‘50’, ‘75’, ‘110’, ‘134’, ‘150’, ‘200’, ‘300’, ‘600’, ‘1200’, ‘1800’, ‘2400’, ‘4800’, ‘9600’, '19200', '38400', '57600', '115200', and '230400'.

Supported parity values are 'None', 'Odd', 'Even', 'Mark' and 'Space'.

Supported data-bits values are '8', '7', '6' and '5'.

Supported stop-bits values are '1', '1.5' and '2'.

Supported flow-control values are 'Hardware', 'Software' and 'None'.

Supported Protocol Configuration

To ensure remote access to serial port 5 is configured as follows:

Telnet Access LAN	Disabled
SSH Access LAN	Enabled
Raw TCP *via* LAN	Disabled

You would need to issue the following commands from the command line to set system configuration:

```
# /bin/config --set=config.ports.port5.ssh=on
# /bin/config --del=config.ports.port5.telnet
# /bin/config --del=config.ports.port5.tcp
```

The following command will synchronize the live system with the new configuration.

```
# /bin/config --run=serialconfig
```

Note: “/bin/config” commands can be combined into one command for convenience.

Users

You can add a User to the system from the command line by following the following instructions:

Determine the total number of existing Users (if you have no existing Users) you can assume this is 0.

```
# /bin/config --get=config.users.total
```

This command should display:

```
config.users.total 1
```

Note that if you see:

```
config.users.total
```

This means you have 0 Users configured.

So your new User will be the existing total plus 1 so if the previous command gave you 0 then you start with user number 1, if you already have 1 user your new user will be number 2 *etc.*

If you want a user named “user1” with a password of “secret” who will have access to serial port 5 from the network you need to issue the these commands (assuming you have a previous user in place):

```
# /bin/config --set=config.users.user2.username=user1
# /bin/config --set=config.users.user2.password=secret
# /bin/config --set=”config.users.user2.description=The Second User”
# /bin/config --set=config.users.user2.port5=on
# /bin/config --set=config.users.total=2
```

The following command will synchronize the live system with the new configuration.

```
# /bin/config --run=users
```

Trusted Networks

You can further restrict remote access to serial ports based on the source IP address. To configure this *via* the command line you need to do the following:

Determine the total number of existing trusted network rules (if you have no existing rules) you can assume this is 0.

```
# /bin/config --get=config.portaccess.total
```

This command should display:

```
config.portaccess.total 1
```

Note that if you see:

```
config.portaccess.total
```

This means you have 0 rules configured.

Your new rule will be the existing total plus 1. So if the previous command gave you 0 then you start with rule number 1. If you already have 1 rule your new rule will be number 2 *etc.*

If you want to restrict access to serial port 5 to computers from a single C class network 192.168.5.0, you need to issue the following commands (assuming you have a previous rule in place):

```
# /bin/config --set=config.portaccess.rule2.address=192.168.5.0
# /bin/config --set=config.portaccess.rule2.netmask=255.255.255.0
# /bin/config --set=”config.portaccess.rule2.description=foo bar.”
```

```
# /bin/config --set=config.portaccess.rule2.port5=on
# /bin/config --set=config.portaccess.total=2
```

Please note that this rule becomes live straight away.

14.6 Event Logging Configuration

Remote Serial Port Log Storage

To setup remote storage of serial port 5 log to a remote Windows share with the following properties:

IP Address	192.168.0.254
Directory	C:\\opengear\logs\
Username	cifs_user
Password	secret
Logging level	2 (input/output logging as well as user connections & disconnections)

The following commands must be issued:

```
# /bin/config --set=config.eventlog.server.type=cifs
# /bin/config --set=config.eventlog.server.address=192.168.0.254
# /bin/config --set=config.eventlog.server.path=/opengear/logs
# /bin/config --set=config.eventlog.server.username=cifs_user
# /bin/config --set=config.eventlog.server.password=secret
# /bin/config --set=config.ports.port5.loglevel=2
```

The following command will synchronize the live system with the new configuration.

```
# /bin/config --run=eventlog
```

Note that supported remote storage server types are 'None', 'cifs', 'nfs' and 'syslog'.

Supported port logging levels are '0', '1' and '2'.

Alert Configuration

You can add an email alert to the system from the command line by following these instructions:

Determine the total number of existing alerts (if you have no existing alerts) you can assume this is 0.

```
# /bin/config --get=config.alerts.total
```

This command should display output similar to:

```
config.alerts.total 1
```

Note that if you see:

```
config.alerts.total
```

This means you have 0 alerts configured.

Your new alert will be the existing total plus 1. So if the previous command gave you 0 then you start with user number 1. If you already have 1 alert your new alert will be number 2 *etc.*

To configure an email alert to be sent to alert1@domain.org when the regular expression “Cpu.*0.0% id,” matches logging on serial port 5 you would need to issue the following commands (Assuming you have 1 previous alert in place):

```
# /bin/config --set=config.alerts.alert2.email=alert1@domain.com
# /bin/config --set=”config.alerts.alert2.pattern=.*0.0% id,”
# /bin/config --set=config.alerts.alert2.port5=on
# /bin/config --del=config.alerts.total=2
```

The following command will synchronize the live system with the new configuration.

```
# /bin/config --run=alerts
```

14.7 SDT Host Configuration

SDT host TCP Ports

To setup the list of tcp ports for a host, you use the config command:

```
# config -s config.sdt.hosts.host3.tcpports.tcport1 = 23
# config -s config.sdt.hosts.host3.tcpports.tcport2 = 5900
# config -s config.sdt.hosts.host3.tcpports.tcport3 = 3389
```

The above assumes the config below:

```
 # vi /etc/config/config.xml ~
             </users>
          </host1>
```

```
            <total>3</total>
            <host2>
               <address>accounts.intranet.myco.com</address>
               <description>Accounts server</description>
               <users>
                  <total>1</total>
                  <user1>JohnWhite</user1>
               </users>
            </host2>
            <host3>
               <address>192.168.254.191</address>
               <description>Tonys Win2000 Box</description>
               <users>
                  <total>1</total>
                  <user1>JohnWhite</user1>
               </users>
               <tcpports><tcpport1>23</tcpport1></tcpports>
            </host3>
         </hosts>
      </sdt>
   </config>
```

Chapter 15 Advanced Configuration

Introduction

This chapter documents Opengear's ***portmanager*** application for gateway serial port management and gives examples of its use:

- *portmanager* documentation
- Scripts and alerts
- Raw data access to the ports and modems

This chapter also describes details how to perform advanced and custom management tasks using Linux commands and script:

- *iptables* modifications and updating IP Filtering rules
- modifying SNMP with *net-snmpd*
- using secure SSH communications
- SSL, configuring HTTPS and issuing certificates
- using the ***pmpower*** application for power device management
- adding new Power Strips and Power Strip control
- using IPMItools
- CDK custom development kit

15.1 Advanced Portmanager

pmshell

The *pmshell* command acts similar to the standard *tip* or *cu* commands, but all serial port access is directed *via* the portmanager.

Example:

To connect to port 8 *via* the portmanager:

```
# pmshell -l port08
```

pmshell Commands:

Once connected, the pmshell command supports a subset of the '~' escape commands that tip/cu support. For SSH you must prefix the escape with an additional '~' command (i.e. use the '~~' escape)

Send Break:

Typing the character sequence '~b' will generate a BREAK on the serial port.

History:

Typing the character sequence '~h' will generate a history on the serial port.

Quit pmshell:

Typing the character sequence '~.' will exit from pmshell.

Set RTS to 1 run the command:

 # pmshell --rts=1

Show all signa

 # pmshell –signals

DSR=1 DTR=1 CTS=1 RTS=1 DCD=0

Read a line of text from the serial port:

 # pmshell –getline

pmchat

The *pmchat* command acts similar to the standard *chat* command, but all serial port access is directed *via* the portmanager.

Example:

To run a chat script *via* the portmanager:

 # pmchat -v -f /etc/config/scripts/port08.chat < /dev/port08

For more information on using *chat* (and *pmchat*) you should consult the UNIX man pages:

http://techpubs.sgi.com/library/tpl/cgi-bin/getdoc.cgi?coll=linux&db=man&fname=/usr/share/catman/man8/chat.8.html

pmusers

The *pmusers* command is used to query the portmanager for active user sessions.

Example:

To detect which users are currently active on which serial ports:

 # pmusers

This command will output nothing if there are no active users currently connected to any ports, otherwise it will respond with a sorted list of usernames per active port:

Port 1:
user1
user2
Port 2:
user1
Port 8:
user2

The above output indicates that a user named "*user1*" is actively connected to ports 1 and 2, while "*user2*" is connected to both ports 1 and 8.

Portmanager Daemon

Command line options

There is normally no need to stop and restart the daemon. To restart the daemon normally, just run the command:

 # portmanager

Supported command line options are:

Force portmanager to run in the foreground:

--nodaemon

Set the level of debug logging:

--loglevel={debug,info,warn,error,alert}

Change which configuration file it uses:

-c /etc/config/portmanager.conf

Signals

Sending a SIGHUP signal to the portmanager will cause it to re-read it's configuration file.

15.2 External Scripts and Alerts

The portmanager has the ability to execute external scripts on certain events. These events are:

I. When a port is opened by the portmanager:

When the portmanager opens a port, it attempts to execute */etc/config/scripts/portXX.init* (where XX is the number of the port, *e.g.* 08). The script is run with STDIN and STDOUT both connected to the serial port.

If the script cannot be executed, then portmanager will execute */etc/config/scripts/portXX.chat via* the chat command on the serial port.

II. When an alert occurs on a port:

When an alert occurs on a port, the portmanager will attempt to execute */etc/config/scripts/portXX.alert* (where XX is the port number, e.g. 08)

The script is run with STDIN containing the data which triggered the alert, and STDOUT redirected to /dev/null, NOT to the serial port. If you wish to communicate with the port, use *pmshell* or *pmchat* from within the script.

If the script cannot be executed, then the alert will be mailed to the address configured in the system administration section.

III. When a user connects to any port:

If a file called */etc/config/pmshell-start.sh* exists it is run when a user connects to a port. It is provided 2 arguments, the "Port number" and the "Username". Here is a simple example:

</etc/config/pmshell-start.sh >

```
#!/bin/sh

PORT="$1"
USER="$2"

echo "Welcome to port $PORT $USER"

< /etc/config/pmshell-start.sh>
```

The return value from the script controls whether the user is accepted or not, if 0 is returned (or nothing is done on exit as in the above script) the user is permitted, otherwise the user is denied access.

Here is a more complex script which reads from configuration to display the port label if available and denies access to the root user:

</etc/config/pmshell-start.sh>

```
#!/bin/sh

PORT="$1"
USER="$2"
LABEL=$(config -g config.ports.port$PORT.label | cut -f2- -d' ')

if [ "$USER" == "root" ]; then
        echo "Permission denied for Super User"
        exit 1
fi

if [  -z  "$LABEL" ]; then
   echo "Welcome $USER, you are connected to Port $PORT"
else
   echo "Welcome $USER, you are connected to Port $PORT ($LABEL)"
```

fi
</etc/config/pmshell-start.sh>

15.3 Raw Access to Serial Ports

Access to Serial Ports

You can *tip* and *stty* to completely bypass the portmanager and have raw access to the serial ports.

When you run *tip* on a portmanager controlled port, portmanager closes that port, and stops monitoring it until tip releases control of it.

With *stty*, the changes made to the port only "stick" until that port is closed and opened again, so it is doubtful that people will want to use *stty* for more than initial debugging of the serial connection.

If you want to use stty to configure the port, you can put *stty* commands in */etc/config/scripts/portXX.init*, which gets run whenever portmanager opens the port.

Otherwise, any setup you do with *stty* will get lost when the portmanager opens the port. (the reason that portmanager sets things back to its *config* rather than using whatever is on the port, is so the port is in a known good state, and will work, no matter what things are done to the serial port outside of portmanager).

Accessing the Console Port

The console dial-in is handled by *mgetty*, with automatic PPP login extensions. *mgetty* is a smart *getty* replacement, designed to be used with hayes compatible data and data/fax modems. *mgetty* knows about modem initialization, manual modem answering (so your modem doesn't answer if the machine isn't ready), UUCP locking (so you can use the same device for dial-in and dial-out). *mgetty* provides very extensive logging facilities. All standard *mgetty* options are supported.

- Modem initialization strings

  To override the standard modem initialization string either use the Management Console (refer *Chapter 5*) or the command line config tool (refer *Dial-In Configuration Chapter 14*).

- Enabling Boot Messages on the Console

  If you are not using a modem on the DB9 console port and instead wish to connect to it directly via a Null Modem cable you may want to enable verbose mode allowing

you to see the standard linux start-up messages. This can be achieved with the following commands:

/bin/config --set=config.console.debug=on # /bin/config --run=console # reboot

If at some point in the future you chose to connect a modem for dial-in out-of-band access the procedure can be reversed with the following commands.

/bin/config --del=config.console.debug # /bin/config --run=console # reboot

15.4 IP- Filtering

Standard IP-Filter configuration:

The system uses the *iptables* utility to provide a stateful firewall of LAN traffic. By default rules are automatically inserted to allow access to enabled services, and serial port access *via* enabled protocols. The commands which add these rules are contained in configuration files.

/etc/config/ipfilter

This is an executable shell script which is run whenever the LAN interface is brought up and whenever modifications are made to the *iptables* configuration as a result of CGI actions or the *config* command line tool.

The basic steps performed are as follows:

a) The current *iptables* configuration is erased.

b) If a customized IP-Filter script exists it is executed and no other actions are performed.

c) Standard policies are inserted which will drop all traffic not explicitly allowed to and through the system.

d) Rules are added which explicitly allow network traffic to access enabled services *e.g.* HTTP, SNMP *etc.*

e) Rules are added which explicitly allow traffic network traffic access to serial ports over enabled protocols *e.g.* Telnet, SSH and raw TCP.

Customizing the IP-Filter:

/etc/config/filter-custom

If the standard system firewall configuration is not adequate for your needs it can be bypassed safely by creating a file at /etc/config/filter-custom containing commands to build a specialized firewall. This firewall script will be run whenever the LAN interface is brought up (including initially) and will override any automated system firewall settings.

Below is a simple example of a custom script which creates a firewall using the *iptables* command. Only incoming connections from computers on a C-class network 192.168.10.0 will be accepted when this script is installed at */etc/config/filter-custom* (Note that when this script is called any preexisting chains and rules have been flushed from *iptables*):

```
#/bin/sh
# Set default policies to drop any incoming or routable traffic
# and blindly accept anything from the 192.168.10.0 network.
iptables --policy FORWARD DROP
iptables --policy INPUT DROP
iptables --policy OUTPUT ACCEPT

# Allow responses to outbound connections back in.
iptables --append INPUT \
     --match state --state ESTABLISHED,RELATED --jump ACCEPT

# Explicitly accept any connections from computers on
# 192.168.10.0/24
iptables --append INPUT --source 192.168.10.0/24 --jump ACCEPT
```

Good documentation about using the *iptables* command can be found at the linux *netfilter* website http://netfilter.org/documentation/index.html

Resources

There are many high-quality tutorials and HOWTOs available *via* the *netfilter* website, in particular peruse the tutorials listed on the *netfilter* HOWTO page. A list of useful web locations has been compiled for your convenience below:

Netfilter Homepage	http://netfilter.org
Netfilter/iptables Tutorials	http://netfilter.org/documentation/index.html#documentation-tutorials

15.5 Modifying SNMP Configuration

/etc/config/snmpd.conf

The *net-snmpd* is an extensible SNMP agent, which when enabled should run with a default configuration. Its behavior can be customized via the options in */etc/config/snmpd.conf.*

Changing standard system information such as system contact, name and location can be achieved by editing */etc/config/snmpd.conf* file and locating the following lines:

```
sysdescr        "opengear"
syscontact      root <root@localhost>(configure
                /etc/default/snmpd.conf)
sysname         Not defined (edit /etc/default/snmpd.conf)
syslocation     Not defined (edit /etc/default/snmpd.conf)
```

Simply change the values of *sysdescr, syscontact, sysname* and *syslocation* to the desired settings and restart *snmpd*.

The *snmpd.conf* provides is extremely powerful and too flexible to completely cover here. The configuration file itself is commented extensively and good documentation is available at the *net-snmp* website http://www.net-snmp.org, specifically:

Man Page:	http://www.net-snmp.org/docs/man/snmpd.conf.html
FAQ:	http://www.net-snmp.org/docs/FAQ.html
Net-SNMPD Tutorial:	http://www.net-snmp.org/tutorial/tutorial-5/demon/snmpd.html

15.6 Secure Shell (SSH) Support

Popular TCP/IP applications such as telnet, rlogin, ftp, and others transmit their passwords unencrypted. Doing this across the Internet can have catastrophic consequences. It leaves the door open for eavesdropping, connection hijacking, and other network-level attacks.

Secure Shell (SSH) is a program to log into another computer over a network, to execute commands in a remote machine, and to move files from one machine to another. It provides strong authentication and secure communications over insecure channels.

OpenSSH, the de facto open source SSH application, encrypts all traffic (including passwords) to effectively eliminate these risks. Additionally, OpenSSH provides a myriad of secure tunneling capabilities, as well as a variety of authentication methods.

OpenSSH is the port of OpenBSD's excellent OpenSSH[0] to Linux and other versions of Unix. OpenSSH is based on the last free version of Tatu Ylonen's sample implementation with all patent-encumbered algorithms removed (to external libraries), all known security bugs fixed, new features reintroduced and many other clean-ups. OpenSSH has been created by Aaron Campbell, Bob Beck, Markus Friedl, Niels Provos, Theo de Raadt, and Dug Song. It has a homepage at http://www.openssh.com/

The only changes in the IMG/IM/CM4000 SSH implementation are:

- PAM support
- EGD[1]/PRNGD[2] support and replacements for OpenBSD library functions that are absent from other versions of UNIX
- The config files are now in */etc/config. e.g.*
    - */etc/config/sshd_config* instead of */etc/sshd_config*
    - */etc/config/ssh_config* instead of */etc/ssh_config*
    - */etc/config/users/<username>/.ssh/* instead of */home/<username>/.ssh/*

Configuring SSH Public Key Authentication (Linux)

This section describes how to generate and configure SSH keys using Linux.

Generating Keys

The following commands can be issued on a Linux host to produce a DSA public/private key pair:

 # ssh-keygen -t dsa

The command will prompt you for a path to store the keys (it will default to ~/.ssh/id_dsa) and a passphrase.

This will produce two files, id_dsa.pub (the public key) and id_dsa (the private key). Full documentation for the ssh-keygen command can be found at:

http://www.openbsd.org/cgi-bin/man.cgi?query=ssh-keygen

Installing Keys

If you have existing SSH keys, you can skip the above Generating Keys step and install them "as is".

The public key can be installed on the unit remotely from the linux host with the scp utility as follows:

Assuming the user on the Management Console is called "fred"; the IP address of the IMG/IM/CM4000 is 192.168.0.1 (default); and the public key is on the *linux/unix* computer in *~/.ssh/id_dsa.pub*. Execute the following command on the *linux/unix* computer:

scp ~/.ssh/id_dsa.pub \root@192.168.0.1:/etc/config/users/fred/.ssh/authorized_keys

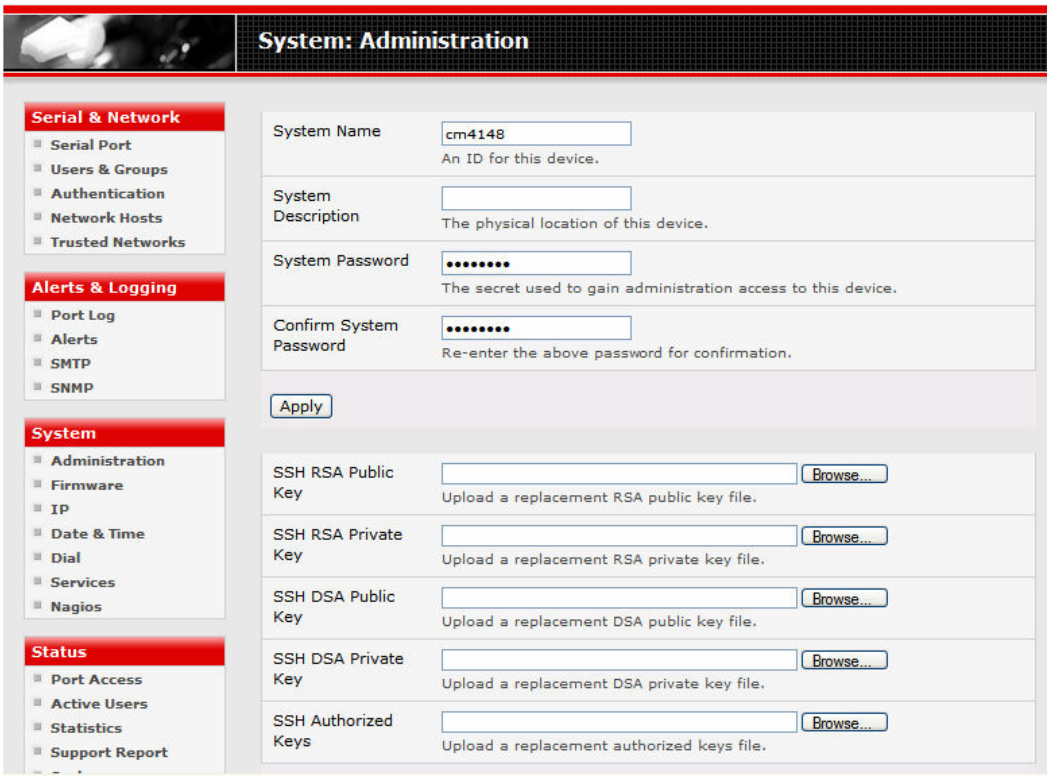
The authorized_keys file on the IMG/IM/CM4000 needs to be owned by "fred", so login to the Management Console as **root** and type:

chown fred /etc/config/users/fred/.ssh/authorized_keys

More documentation on OpenSSH can be found at:

http://openssh.org/portable.html
http://www.openbsd.org/cgi-bin/man.cgi?query=ssh&sektion=1
http://www.openbsd.org/cgi-bin/man.cgi?query=sshd

For Opengear gateways with firmware post V2.2.3, the keys can be simply uploaded through the web interface, on the **System: Administration** page:



Generating non-interactive public/private keys for SSH (Windows)

This section describes how to generate and configure SSH keys using Windows.

First create a new user from the Opengear Management Console on Opengear gateway (the following example users a user called "testuser") making sure it is a member of the "users" group.

If you do not already have a public/private key pair you can generate them now using *ssh-keygen*, *PuTTYgen* or a similar tool:

PuTTYgen:
http://www.chiark.greenend.org.uk/~sgtatham/putty/download.html

OpenSSH:
http://www.openssh.org/

OpenSSH (Windows):
http://sshwindows.sourceforge.net/download/

For example using PuTTYgen, make sure you have a recent version of the *puttygen.exe* (available from http://www.chiark.greenend.org.uk/~sgtatham/putty/download.html) Make sure you have a recent version of WinSCP (available from http://winscp.net/eng/download.php)

Field Code Changed

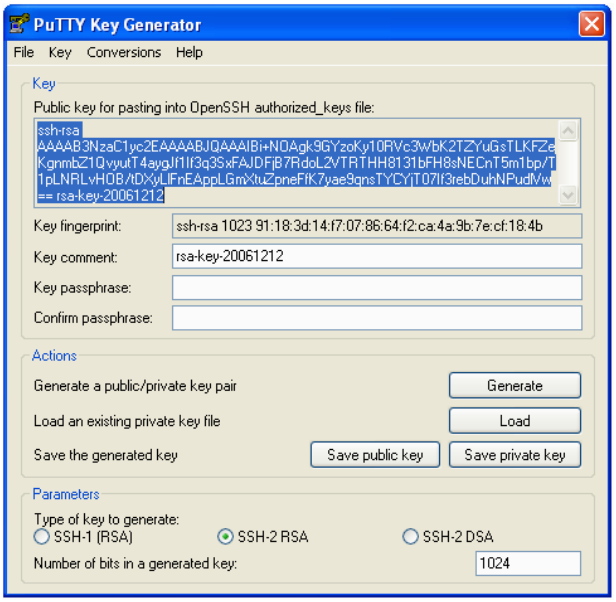
Field Code Changed

To generate a SSH key using PuTTY http://sourceforge.net/docs/F02/#clients:

Field Code Changed

- Execute the PUTTYGEN.EXE program
- Select the desired key type *SSH2 DSA* (you may use RSA or DSA) within the *Parameters* section
- It is important that you leave the passphrase field blank
- Click on the *Generate* button
- Follow the instruction to move the mouse over the blank area of the program in order to create random data used by PUTTYGEN to generate secure keys. Key generation will occur once PUTTYGEN has collected sufficient random data

.



- Create a new file " *authorized_keys* " (with notepad) and copy your public key data from the "Public key for pasting into OpenSSH authorized_keys file" section of the PuTTY Key Generator, and paste the key data to the "authorized_keys" file. Make sure there is only one line of text in this file.

- Use WinSCP to copy this "authorized_keys" file into the users home directory: eg. */etc/config/users/testuser/.ssh/authorized_keys* of the Opengear gateway which will be the SSH server. You will need to make sure this file is in the correct format with the correct permissions with the following commands:

  *# dos2unix *
  */etc/config/users/testuser/.ssh/authorized_keys && chown testuser *
  /etc/config/users/testuser/.ssh/authorized_keys

- Using WinSCP copy the attached sshd_config over */etc/config/sshd_config* on the server (Makes sure public key authentication is enabled)

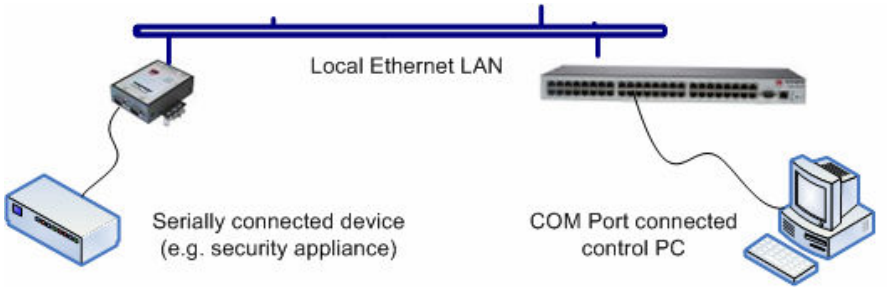
- Test the Public Key by logging in as "testuser" Test the Public Key by logging in as "testuser" to the client Opengear device and typing (you should not need to enter anything): # ssh -o StrictHostKeyChecking=no <server-ip>

To automate connection of the SSH tunnel from the client on every power-up you need to make the clients /etc/config/rc.local look like the following:
#!/bin/sh
ssh -L9001:127.0.0.1:4001 -N -o StrictHostKeyChecking=no testuser@<server-ip> &

This will run the tunnel redirecting local port 9001 to the server port 4001.

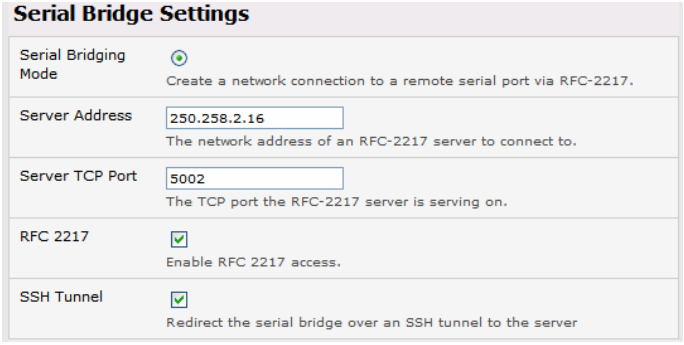
SSH tunneled serial bridging

You have the option to apply SSH tunneling when two Opengear gateways are configured for serial bridging.



As detailed in *Chapter 4*, the *Server* gateway is setup in Console Server mode with either RAW or RFC2217 enabled and the *Client* gateway is set up in Serial Bridging Mode with the Server Address, and Server TCP Port (4000 + port for RAW or 5000 + port # for RFC2217) specified:

- Select **SSH Tunnel** when configuring the **Serial Bridging Setting**



Next you will need to set up SSH keys for each end of the tunnel and upload these keys to the *Server* and *Client* gateways.

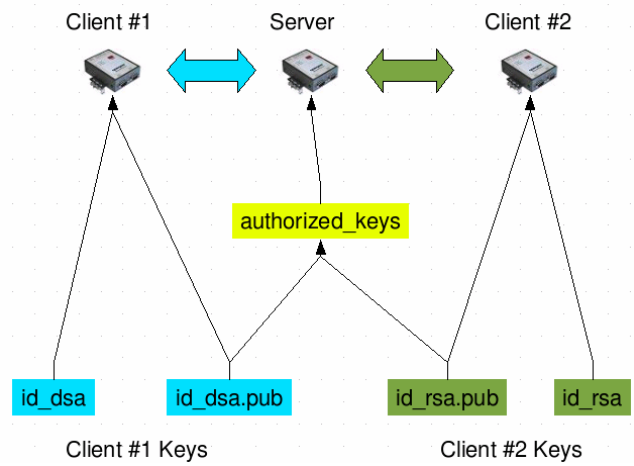
Client Keys

The first step in setting up ssh tunnels is to generate keys. Ideally, you will use a separate, secure, machine to generate and store all keys to be used on the Opengear devices. However, if this is not ideal to your situation, keys may be generated on the Opengear boxes themselves.

It is possible to generate only one set of keys, and reuse them for every SSH session. While this is not recommended, each organization will need to balance the security of separate keys against the additional administration they bring.

Generated keys may be one of two types - RSA or DSA (and it is beyond the scope of this document to recommend one over the other). RSA keys will go into the files *id_rsa* and *id_rsa.pub*. DSA keys will be stored in the files *id_dsa* and *id_dsa.pub*.

For simplicity going forward the term *private key* will be used to refer to either *id_rsa* or *id_dsa* and *public key* to refer to either *id_rsa.pub* or *id_dsa.pub*.



To generate the keys using OpenBSD's OpenSSH suite, we use the *ssh-keygen* program:

$ ssh-keygen -t [rsa|dsa]
Generating public/private [rsa|dsa] key pair.
Enter file in which to save the key *(/home/user/.ssh/id_[rsa|dsa]):*
Enter *passphrase* (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in */home/user/.ssh/id_[rsa|dsa].*
Your public key has been saved in */home/user/.ssh/id_[rsa|dsa].pub.*
The key fingerprint is:
28:aa:29:38:ba:40:f4:11:5e:3f:d4:fa:e5:36:14:d6 user@server
$

It is advisable to create a new directory to store your generated keys. It is also possible to name the files after the device they will be used for. For example:

$ mkdir keys
$ ssh-keygen -t rsa
Generating public/private rsa key pair.
Enter file in which to save the key (/home/user/.ssh/id_rsa):
/home/user/keys/control_room
Enter *passphrase* (empty for no passphrase):
Enter same *passphrase* again:
Your identification has been saved in */home/user/keys/control_room*
Your public key has been saved in */home/user/keys/control_room.pub*.
The key fingerprint is:
28:aa:29:38:ba:40:f4:11:5e:3f:d4:fa:e5:36:14:d6 user@server
$

You should ensure there is no password associated with the keys. If there is a password, then the Opengear devices will have no way to supply it as runtime.

Authorized Keys

If the Opengear device selected to be the server will only have one client device, then the *authorized_keys* file is simply a copy of the public key for that device. If one or more devices will be clients of the server, then the *authorized_keys* file will contain a copy of all of the public keys. RSA and DSA keys may be freely mixed in the *authorized_keys* file.

For example, assume we already have one server, called *bridge_server*, and two sets of keys, for the *control_room* and the *plant_entrance*:

$ ls /home/user/keys
control_room control_room.pub plant_entrance plant_entrance.pub
$ cat /home/user/keys/control_room.pub
/home/user/keys/plant_entrance.pub >
/home/user/keys/authorized_keys_bridge_server

Uploading Keys

The keys for the server can be uploaded through the web interface, on the **System: Administration** page as detailed earlier. If only one client will be connecting, then simply upload the appropriate public key as the authorized keys file. Otherwise, upload the authorized keys file constructed in the previous step.

Each client will then need it's own set of keys uploaded through the same page. Take care to ensure that the correct type of keys (DSA or RSA) go in the correct spots, and that the public and private keys are in the correct spot.

SDTConnector Public Key Authentication

SDTConnector can authenticate against a Opengear gateway using your SSH key pair rather than requiring your to enter your password (i.e. public key authentication).

- To use public key authentication with SDTConnector, first you must first create an RSA or DSA key pair (using *ssh-keygen, PuTTYgen* or a similar tool) and add the public part of your SSH key pair to the Opengear gateway – as described in the earlier section.

- Next, add the private part of your SSH key pair (this file is typically named *id_rsa* or *id_dsa*) to SDTConnector client. Click **Edit -> Preferences -> Private Keys -> Add**,

locate the private key file and click **OK**. You do not have to add the public part of your SSH key pair, it is calculated using the private key.

SDTConnector will now use public key authentication when SSH connecting through the IMG/IM/CM4000 gateway. You may have to restart SDTConnector to shut down any existing tunnels that were established using password authentication.

If you have a host behind the IMG/IM/CM4000 gateway that you connect to by clicking the SSH button in SDTConnector, you can also configure it for public key authentication. Essentially what you are using is SSH over SSH, and the two SSH connections are entirely separate, and the host configuration is entirely independent of SDTConnector and the IMG/IM/CM4000 gateway. You must configure the SSH client that SDTConnector launches (e.g. Putty, OpenSSH) and the host's SSH server for public key authentication.

15.7 Secure Sockets Layer (SSL) Support

Secure Sockets Layer (SSL) is a protocol developed by Netscape for transmitting private documents *via* the Internet. SSL works by using a private key to encrypt data that's transferred over the SSL connection.

The IMG/IM/CM4000 includes OpenSSL. The OpenSSL Project is a collaborative effort to develop a robust, commercial-grade, full-featured, and Open Source toolkit implementing the Secure Sockets Layer (SSL v2/v3) and Transport Layer Security (TLS v1) protocols as well as a full-strength general purpose cryptography library. The project is managed by a worldwide community of volunteers that use the Internet to communicate, plan, and develop the OpenSSL toolkit and its related documentation.

OpenSSL is based on the excellent SSLeay library developed by Eric A. Young and Tim J. Hudson. The OpenSSL toolkit is licensed under an Apache-style licence, which basically means that you are free to get and use it for commercial and non-commercial purposes subject to some simple license conditions. In the IMG/IM/CM4000 OpenSSL is used primarily in conjunction with ‘http’ in order to have secure browser access to the GUI management console across insecure networks.

More documentation on OpenSSL is available from:

http://www.openssl.org/docs/apps/openssl.html

http://www.openssl.org/docs/HOWTO/certificates.txt

15.8 HTTPS

The Management Console can be served using HTTPS by running the webserver *via sslwrap*. The server can be launched on request using *inetd*.

The HTTP server provided is a slightly modified version of the *fnord-httpd* from http://www.fefe.de/fnord/

The SSL implementation is provided by the *sslwrap* application compiled with OpenSSL support. More detailed documentation can be found at http://www.rickk.com/sslwrap/

If your default network address is changed or the unit is to be accessed *via* a known Domain Name you can use the following steps to replace the default SSL Certificate and Private Key with ones tailored for your new address.

1. Generating an encryption key

To create a 1024 bit RSA key with a password issue the following command on the command line of a linux host with the *openssl* utility installed:

openssl genrsa -des3 -out ssl_key.pem 1024

2. Generating a self-signed certificate with OpenSSL

This example shows how to use OpenSSL to create a self-signed certificate. OpenSSL is available for most Linux distributions *via* the default package management mechanism. (Windows users can check http://www.openssl.org/related/binaries.html)

To create a 1024 bit RSA key and a self-signed certificate issue the following *openssl* command from the host you have *openssl* installed on:

*openssl req -x509 -nodes -days 1000 *
-newkey rsa:1024 -keyout ssl_key.pem -out ssl_cert.pem

You will be prompted to enter a lot of information. Most of it doesn't matter, but the "Common Name" should be the domain name of your computer (*e.g.* test.opengear.com). When you have entered everything, the certificate will be created in a file called *ssl_cert.pem*.

3. Installing the key and certificate

The recommended method for copying files securely to the IMG/IM/CM4000 unit is with an SCP (Secure Copying Protocol) client. The *scp* utility is distributed with OpenSSH for

most Unices, while Windows users can use something like the PSCP command line utility available with PuTTY.

The files created in steps 1 and 2 can be installed remotely with the *scp* utility as follows:

scp ssl_key.pem root@<address of unit>:/etc/config/
scp ssl_cert.pem root@<address of unit>:/etc/config/

or using PSCP:

pscp -scp ssl_key.pem root@<address of unit>:/etc/config/
pscp -scp ssl_cert.pem root@<address of unit>:/etc/config/

PuTTY and the PSCP utility can be downloaded from
http://www.chiark.greenend.org.uk/~sgtatham/putty/download.html

More detailed documentation on the PSCP can be found:
http://the.earth.li/~sgtatham/putty/0.58/htmldoc/Chapter5.html#pscp

4. Launching the HTTPS Server

Note that the easiest way to enable the HTTPS server is from the web Management Console. Simply click the apropriate checkbox in **Network -> Services -> HTTPS Server** and the HTTPS server will be activated (assuming the *ssl_key.pem* & *ssl_cert.pem* files exist in the */etc/config* directory).

Alternatively *inetd* can be configured to launch the secure fnord server from the command line of the unit as follows.

Edit the *inetd* configuration file. From the unit command line:

vi /etc/config/inetd.conf

Append a line:

443 stream tcp nowait root sslwrap -cert /etc/config/ssl_cert.pem -key /etc/config/ssl_key.pem -exec /bin/httpd /home/httpd"

Save the file and signal *inetd* of the configuration change.

kill -HUP `cat /var/run/inetd.pid`

The HTTPS server should be accessible from a web client at a URL similar to this: https://<common name of unit>

More detailed documentation about the *openssl* utility can be found at the website: http://www.openssl.org/

15.9 Power Strip Control

The IMG/IM/CM4000 supports a limited set of power-control devices which can be configured using the Management Console as described in Chapter 8.

pmpower

The *pmpower* command is a high level tool for manipulating remote preconfigured power devices connected to the Opengear gateway either via a serial or network connection.

Example:

To turn outlet 4 of the power device connected to serial port 2 on:

pmpower -l port02 -o 4 on

To turn an IPMI device off located at IP address 192.168.1.100 (where username is 'root' and password is 'calvin':

 # pmpower -r 192.168.1.100 -u root -p calvin off

pmpower Actions:

pmpower supports the following possible actions:

on: Turn the device (or outlet) on.

off: Turn the device (or outlet) off.

cycle: Turn the device (or outlet) off then back on.

status: Retrieve the current status of the specified power device (or outlet).

Default system Power Device actions are specified in */etc/powerstrips.xml*, custom Power Devices can be added in */etc/config/powerstrips.xml*. If an action is attempted

which has not been configured for a specific Power Device *pmpower* will exit with an error.

Adding new Power Devices

It is fairly simple to add support for more devices, or to customize the existing device support. The **Administration: Power** page uses information contained in */etc/powerstrips.xml* to configure and control devices attached to a serial port. The configuration also looks for (and loads) */etc/config/powerstrips.xml* if it exists.

The user can add their own support for more devices by putting definitions for them into */etc/config/powerstrips.xml*. This file can be created on a host system and copied to the Management Console device using *scp*. Alternatively, login to the Management Console and use *ftp* or *wget* to transfer files.

Here is a brief description of the elements of the XML entries in */etc/config/powerstrips.xml*.

<powerstrip>

<id>Name or ID of the device support</id>

<outlet port="port-id-1">Display Port 1 in menu</outlet>

<outlet port="port-id-2">Display Port 2 in menu</outlet>

...

<on>script to turn power on</on>

<off>script to power off</off>

<cycle>script to cycle power</cycle>

<status>script to write power status to /var/run/power-status</status>

<speed>baud rate</speed>

<charsize>character size</charsize>

<stop>stop bits</stop>

<parity>parity setting</parity>

</powerstrip>

The *id* appears on the web page in the list of available devices types to configure.

The outlets describe targets that the scripts can control. For example a power control board may control several different outlets. The port-id is the native name for identifying the outlet. This value will be passed to the scripts in the environment variable *outlet*, allowing the script to address the correct outlet.

There are four possible scripts: *on, off, cycle* and *status*

When a script is run, it's standard input and output is redirected to the appropriate serial port. The script receives the outlet and port in the *outlet* and *port* environment variables respectively.

The script can be anything that can be executed within the shell.

All of the existing scripts in */etc/powerstrips.xml* use the *pmchat* utility.

pmchat works just like the standard unix "chat" program, only it ensures

interoperation with the port manager.

The final options, *speed, charsize, stop* and *parity* define the recommended or default settings for the attached device.

15.10 IPMItool

The IMG/IM/CM4000 includes the *ipmitool* utility for managing and configuring devices that support the Intelligent Platform Management Interface (IPMI) version 1.5 and version 2.0 specifications.

IPMI is an open standard for monitoring, logging, recovery, inventory, and control of hardware that is implemented independent of the main CPU, BIOS, and OS. The service processor (or Baseboard Management Controller, BMC) is the brain behind platform management and its primary purpose is to handle the autonomous sensor monitoring and event logging features.

The *ipmitool* program provides a simple command-line interface to this BMC. It features the ability to read the sensor data repository (SDR) and print sensor values, display the contents of the System Event Log (SEL), print Field Replaceable Unit (FRU) inventory information, read and set LAN configuration parameters, and perform remote chassis power control.

SYNOPSIS

ipmitool [**-c**|**-h**|**-v**|**-V**] **-I** *open* <*command*>

ipmitool [**-c**|**-h**|**-v**|**-V**] **-I** *lan* **-H** <*hostname*>
[**-p** <*port*>]
[**-U** <*username*>]
[**-A** <*authtype*>]
[**-L** <*privlvl*>]
[**-a**|**-E**|**-P**|**-f** <*password*>]
[**-o** <*oemtype*>]
<*command*>

ipmitool [**-c**|**-h**|**-v**|**-V**] **-I** *lanplus* **-H** <*hostname*>
[**-p** <*port*>]
[**-U** <*username*>]
[**-L** <*privlvl*>]
[**-a**|**-E**|**-P**|**-f** <*password*>]
[**-o** <*oemtype*>]
[**-C** <*ciphersuite*>]
<*command*>

DESCRIPTION

This program lets you manage Intelligent Platform Management Interface (IPMI) functions of either the local system, via a kernel device driver, or a remote system, using IPMI V1.5 and IPMI v2.0. These functions include printing FRU information, LAN configuration, sensor readings, and remote chassis power control.

IPMI management of a local system interface requires a compatible IPMI kernel driver to be installed and configured. On Linux this driver is called *OpenIPMI* and it is included in standard distributions. On Solaris this driver is called *BMC* and is inclued in Solaris 10. Management of a remote station requires the IPMI-over-LAN interface to be enabled and configured. Depending on the particular requirements of each system it may be possible to enable the LAN interface using *ipmitool* over the system interface.

OPTIONS

-a Prompt for the remote server password.

-A <*authtype*>
Specify an authentication type to use during IPMIv1.5 *lan* session activation. Supported types are NONE, PASSWORD, MD5, or OEM.

-c Present output in CSV (comma separated variable) format. This is not available with all commands.

-C <*ciphersuite*>
The remote server authentication, integrity, and encryption algorithms to use for IPMIv2 *lanplus* connections. See table 22-19 in the IPMIv2 specification. The default is 3 which specifies RAKP-HMAC-SHA1 authentication, HMAC-SHA1-96 integrity, and AES-CBC-128 encryption algorightms.

-E The remote server password is specified by the environment variable *IPMI_PASSWORD*.

-f <*password_file*>
Specifies a file containing the remote server password. If this option is absent, or if password_file is empty, the password will default to NULL.

-h Get basic usage help from the command line.

-H <*address*>
Remote server address, can be IP address or hostname. This option is required for *lan* and *lanplus* interfaces.

-I <*interface*>
Selects IPMI interface to use. Supported interfaces that are compiled in are visible in the usage help output.

-L <*privlvl*>
Force session privilege level. Can be CALLBACK, USER, OPERATOR, ADMIN. Default is ADMIN.

-m <*local_address*>
Set the local IPMB address. The default is 0x20 and there should be no need to change it for normal operation.

-o <*oemtype*>

Select OEM type to support. This usually involves minor hacks in place in the code to work around quirks in various BMCs from various manufacturers. Use *-o list* to see a list of current supported OEM types.

-p <*port*>
Remote server UDP port to connect to. Default is 623.

-P <*password*>
Remote server password is specified on the command line. If supported it will be obscured in the process list. **Note!** Specifying the password as a command line option is not recommended.

-t <*target_address*>
Bridge IPMI requests to the remote target address.

-U <*username*>
Remote server username, default is NULL user.

-v Increase verbose output level. This option may be specified multiple times to increase the level of debug output. If given three times you will get hexdumps of all incoming and outgoing packets.

-V Display version information.

If no password method is specified then *ipmitool* will prompt the user for a password. If no password is entered at the prompt, the remote server password will default to NULL.

SECURITY

The *ipmitool* documentation highlights that there are several security issues to be considered before enabling the IPMI LAN interface. A remote station has the ability to control a system's power state as well as being able to gather certain platform information. To reduce vulnerability it is strongly advised that the IPMI LAN interface only be enabled in 'trusted' environments where system security is not an issue or where there is a dedicated secure 'management network' or access has been provided through an IMG/IM/CM4000.

Further it is strongly advised that you should not enable IPMI for remote access without setting a password, and that that password should not be the same as any other password on that system.

When an IPMI password is changed on a remote machine with the IPMIv1.5 *lan* interface the new password is sent across the network as clear text. This could be observed and then used to attack the remote system. It is thus recommended that IPMI password management only be done over IPMIv2.0 *lanplus* interface or the system interface on the local station.

For IPMI v1.5, the maximum password length is 16 characters. Passwords longer than 16 characters will be truncated.

For IPMI v2.0, the maximum password length is 20 characters; longer passwords are truncated.

COMMANDS

help

This can be used to get command-line help on *ipmitool* commands. It may also be placed at the end of commands to get option usage help.

ipmitool help

Commands:

raw	Send a RAW IPMI request and print response
lan	Configure LAN Channels
chassis	Get chassis status and set power state
event	Send pre-defined events to MC
mc	Management Controller status and global enables
sdr	Print Sensor Data Repository entries and readings
sensor	Print detailed sensor information
fru	Print built-in FRU and scan SDR for FRU locators
sel	Print System Event Log (SEL)
pef	Configure Platform Event Filtering (PEF)
sol	Configure IPMIv2.0 Serial-over-LAN
isol	Configure IPMIv1.5 Serial-over-LAN
user	Configure Management Controller users
channel	Configure Management Controller channels
session	Print session information
exec	Run list of commands from file
set	Set runtime variable for shell and exec

ipmitool chassis help

Chassis Commands: status, power, identify, policy, restart_cause, poh, bootdev

ipmitool chassis power help

chassis power Commands: status, on, off, cycle, reset, diag, soft

You will find more details on *ipmitools* at http://*ipmitool*.sourceforge.net/manpage.html

15.11 Custom Development Kit (CDK)

As detailed in this manual customers can copy scripts, binaries and configuration files directly to the IMG/IM/CM4000.

Opengear also freely provides a development kit which allows changes to be made to the software in IMG/IM/CM4000 firmware image. The customer can use the CDK to:

- generate a firmware image without certain programs, such as telnet, which may be banned by company policy
- generate an image with new programs, such as custom Nagios plugin binaries or company specific binary utilities
- generate an image with custom defaults e.g. it may be required that the IMG/IM/CM4000 be configured to have a specific default serial port profile which is reverted to even in event of a factory reset
- place configuration files into the firmware image, which cannot then be modified e.g. # /bin/config –-set= tools update the configuration files in /etc/config which are read/write, whereas the files in /etc are read only and cannot be modified

The CDK essentially provides a snapshot of the Opengear build process (taken after the programs have been compiled and copied to a temporary directory *romfs*) just before the compressed file systems are generated. You can obtain a copy of the Opengear CDK for the particular appliance you are working with from ftp://ftp.opengear.com/cdk and find further information online at http://www.opengear.com/faq284.html

Note The CDK is free, however Opengear does not provide free technical support for systems modified using the CDK and any changes are the responsibility of the user.

Appendix A Linux Kernel and Source Code

The IMG/IM/CM4000 platform is a dedicated Linux computer, optimized to provide secure access to serial consoles of critical server systems. Being based around uClinux (a small footprint but extensible Linux), it embodies a myriad, popular and proven Linux software modules for networking (NetFilter, IPTables), secure access (OpenSSH) and communications (OpenSSL) and sophisticated user authentication (PAM, RADIUS, TACACS+ and LDAP).

Many components of the IMG/IM/CM4000 software are licensed under the GNU General Public License (version 2), which Opengear supports. You may obtain a copy of the GNU General Public License at http://www.fsf.org/copyleft/gpl.html. Opengear will provide source code for any of the components of the Software licensed under the GNU General Public License upon request.

Opengear IMG/IM/CM4000 gateways are built on the 2.4 uClinux kernel as developed by the uClinux project. This is GPL code and source can be found: http://cvs.uclinux.org

Commands that have config files that can be altered:

portmanager
inetd
init
ssh/sshd/scp/sshkeygen
ucd-snmpd http://www.ece.ucdavis.edu/ucd-snmp/
samba
fnord (web server)
sslwrap

Commands you can run and do neat stuff with are:

loopback
bash (shell)
busybox http://www.busybox.net/downloads/BusyBox.html
(has lots of unix shell commands and tools)
chat
dhcpcd
ftp
hd
hwclock

iproute
iptables
netcat
ifconfig
mii-tool
netstat
route
openntpd
ping
portmap
pppd
routed
setserial
smtpclient
stty
stunel
tcpdump
tftp
tip
traceroute

A full list of the Linux commands and applications included in the latest IMG/IM/CM4000 build can be found at http://www.opengear.com/faq233.html

More details on the Linux commands can found online at:

http://en.tldp.org/HOWTO/HOWTO-INDEX/howtos.html

http://www.faqs.org/docs/Linux-HOWTO/Remote-Serial-Console-HOWTO.html

http://www.stokely.com/unix.serial.port.resources/serial.switch.html

The IMG/IM/CM4000 also embodies the *okvm* console management software. This is GPL code and the full source is available from http://okvm.sourceforge.net.

The IMG/IM/CM4000 BIOS (boot loader code) is a port of uboot which is also a GPL package with source openly available.

The IMG/IM/CM4000 CGIs (the html code, xml code and web config tools for the Console Manager) are proprietary to Opengear, however the code will be provided to customers, under NDA.

Also inbuilt in the IMG/IM/CM4000 is a Port Manager application and Configuration tools as described in Chapters 11 and 12. These both are proprietary to Opengear, but open to customers (as above).

Appendix B Hardware Specifications

FEATURE	VALUE
Dimensions	IM4208/16/48: 17 x 12 x 1.75 in (43.2 x 31.3. x 4.5 cm) IMG4216-25: 17 x 12 x 1.75 in (43.2 x 31.3. x 4.5 cm) IMG4004-5: 8.2 x 4.9 x 1.2 in (20.8 x 12.6 x 4.5 cm) CM4116/48: 17 x 8.5 x 1.75 in (43.2 x 21. x 4.5 cm) CM4008: 8.2 x 4.9 x 1.2 in (20.8 x 12.6 x 4.5 cm) CM4001: 3.9 x 2.8 x 1.0 in (10 x 7.2 x 2.5 cm)
Weight	IM4208/16/48: 5.4 kg (11.8 lbs) IMG4216-25: 5.4 kg (11.8 lbs) IMG4004-5: 1.7 kg (3.7 lbs) CM4116/48: 3.9 kg (8.5 lbs) CM4008:1.7 kg (3.7 lbs) CM4001: 1.1 kg (2.5 lbs)
Ambient operating temperature	5°C to 50°C (41°F to 122°F)
Non operating storage temperature	-30°C to +60°C (-20°F to +140°F)
Humidity	5% to 90%
Power	Refer Chapter 2 for various models
Power Consumption	All less than 30W
CPU	Micrel KS8695P controller
Memory	IM4208/16/48: 64MB SDRAM 16MB Flash 512MB USB Flash IM4248-2: 64MB SDRAM 16MB Flash 512MB USB Flash IMG4004-5: 64MB SDRAM 16MB Flash 1G USB Flash CM4116/48: 64MB SDRAM 16MB Flash

	CM4008: 16MB SDRAM 8MB Flash CM4001: 16MB SDRAM 8MB Flash
Serial Connectors	IM4208-2: 8 RJ-45 RS-232 serial ports IM4216-2: 16 RJ-45 RS-232 serial ports IM4248-2: 48 RJ-45 RS-232 serial ports IMG4004-5: 4 RJ-45 RS-232 serial ports IMG4216-25: 16 RJ-45 RS-232 serial ports CM4116: 16 RJ-45 RS-232 serial ports CM4148: 48 RJ-45 RS-232 serial ports CM4008: 8 RJ-45 RS-232 serial ports CM4001: 1 DB-9 RS-232 serial port All models: 1 DB-9 RS-232 console/ modem serial port
Serial Baud Rates	RJ45 ports - 50 to 230,400bps) DB9 port - 2400 to 115,200 bps
Ethernet Connectors	IM4208/16/48-2: Two RJ-45 10/100Base-T Ethernet ports IMG4216-25: One RJ-45 10/100Base-T primary Ethernet port and 24 RJ-45 10/100Base-T management LAN switched ports IMG4004-5: One RJ-45 10/100Base-T primary Ethernet port and 4 RJ-45 10/100Base-T management LAN switched ports CM41xx One RJ-45 10/100Base-T Ethernet ports

Appendix C Safety & Certifications

Please take care to follow the safety precautions below when installing and operating the IMG/IM/CM4000:

- Do not remove the metal covers. There are no operator serviceable components inside. Opening or removing the cover may expose you to dangerous voltage which may cause fire or electric shock. Refer all service to Opengear qualified personnel
- To avoid electric shock the power cord protective grounding conductor must be connected through to ground.
- Always pull on the plug, not the cable, when disconnecting the power cord from the socket.

Do not connect or disconnect the IMG/IM/CM4000 during an electrical storm. Also it is recommended you use a surge suppressor or UPS to protect the equipment from transients.

FCC Warning Statement

This device complies with Part 15 of the FCC rules. Operation of this device is subject to the following conditions: (1) This device may not cause harmful interference, and (2) this device must accept any interference that may cause undesired operation.

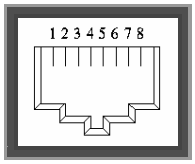
Appendix D Connectivity and Serial I/O

Pinout standards exist for both DB9 and DB25 connectors; however there are not pinout standards for serial connectivity using RJ45 connectors. Most console servers and serially managed servers/ router/ switches/ PSUs have adopted their own unique pinout; so custom connectors and cables may be required to interconnect your IMG/IM/CM4000.

In an endeavor to create some move to standardization, Opengear products all use the same RJ45 pinout convention as adopted by Avocent and Equinox.

Serial Port Pinout

The 8/16/48 RJ45 connectors on the CM4008/4116/4148 and IM4216/4248 unit have the following pinout:

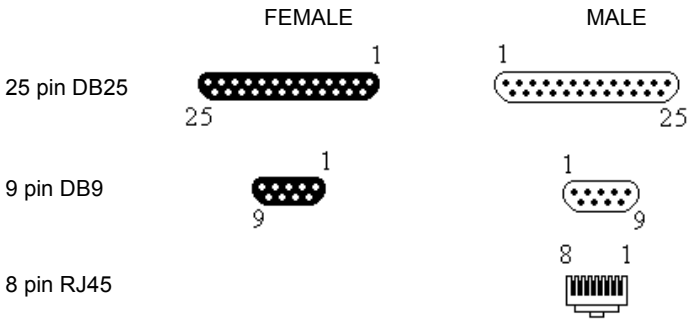


Pin	Signal	Direction	RS232 Signal Description
1	RTS	Output	Request To Send
2	DSR	Input	Data Set Ready
3	DCD	Input	Data Carrier Detect
4	RXD	Input	Receive Data
5	TXD	Output	Transmit Data
6	GND	NA	Ground
7	DTR	Output	Data Terminal Ready
8	CTS	Input	Clear To Send

The LOCAL (console/modem) port on the IMG/IM/CM4000 uses a standard DB9 connector, as does the serial port on the CM4001. The RS232 pinout standards for the DB9 (and DB25) connectors are tabled below:

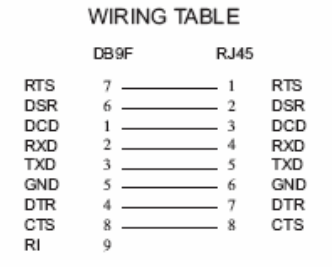
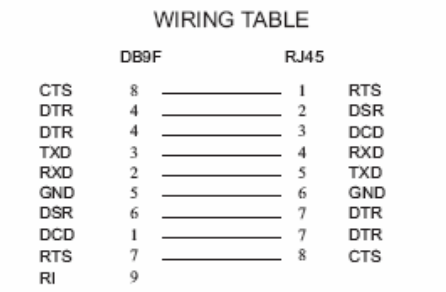
DB25	SIGNAL	DB9	DEFINITION
1			Protective Ground
2	TXD	3	Transmitted Data
3	RXD	2	Received Data
4	RTS	7	Request To Send
5	CTS	8	Clear To Send
6	DSR	6	Data Set Ready

7	GND	5	Signal Ground
8	CD	1	Received Line Signal Detector
9			Reserved for data set testing
10			Reserved for data set testing
11			Unassigned
12	SCF		Secondary Rcvd Line Signal Detector
13	SCB		Secondary Clear to Send
14	SBA		Secondary Transmitted Data
15	DB		Transmission Signal Timing
16	SBB		Secondary Received Data
17	DD		Receiver Signal Element Timing
18			Unassigned
19	SCA		Secondary Request to Send
20	DTR	4	Data Terminal Ready
21	CG		Signal Quality Detector
22		9	Ring Indicator
23	CH/CI		Data Signal Rate Selector
24	DA		Transmit Signal Element Timing
25			Unassigned



Connectors included in IMG/IM/CM4000

The CM4008/4116/4148 and IM4208/16/48 all ship with a “cross-over” and a “straight” RJ45-DB9 connector for connecting to other vendor’s products:

 Part # 319000	DB9F-RJ45S straight connector	
 Part # 319001	DB9F-RJ45S cross-over connector	

Other available connectors and adapters

Opengear also supplies a range of cables and adapters that will enable you to easily connect to the more popular servers and network appliances. More detailed information can be found online at http://www.opengear.com/cabling.html

- Local/Console connection

These adapters connect the IMG/IM/CM4000 LOCAL/Console port (via standard UTP Cat 5 cable) to modem devices (for out-of-band access):

319000	DB9F to RJ45 straight	IMG/IM/CM4000 LOCAL Console Port to Modem
319002	DB25M to RJ45 straight	IMG/IM/CM4000 LOCAL Console Port to Modem

- IMG/IM/CM4000 Serial Port connection

The connectors and adapters in the table below all work with standard UTP Cat 5 cables:

319001	DB9F to RJ45 crossover	DCE Adapter - IMG/IM/CM4000 Ports to X86 and other

319002	DB25M to RJ45 straight	DTE Adapter - IMG/IM/CM4000 Ports
319003	DB25M to RJ45 crossover	DCE Adapter - IMG/IM/CM4000 Ports to Sun and other
319004	DB9M to RJ45 straight	DTE Adapter - IMG/IM/CM4000 to Netscreen and Dell
319005	DB25F to RJ45 crossover	DCE Adapter - IMG/IM/CM4000 to Cisco 7200 AUX
440016	5ft Cat5 RJ-45 to RJ-45 cables	Extension cables
449016	RJ-45 Plug to RJ-45 Jack	Adapter for Cisco console

Appendix E Hardware Test

This section describes the Loopback Test facilities built into the IMG/IM/CM4000 code. When undertaking a Loopback Test, each of the serial ports loop data transmitted to data received, RTS to CTS, and DTR to DSR + DCD. The loopback program senses that data sent is received properly and that signals set and received properly. The Loopback Test also undertakes an Ethernet loopback that senses the data transmitted is received properly.

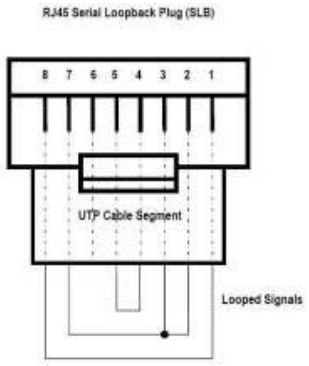
To undertake these tests you must have at hand:

- IMG/IM/CM4000 unit (CM4008,CM4116 or CM4148)
- Terminal device (*e.g.* Windows PC and HyperTerminal program)
- Serial console cabling *e.g.* UTP Cat5 cable (#440016), DB-9 to RJ45 DTE adapter (#319000) and DB-9 to RJ45 DCE adapter (#319001)
- Custom made R-45 serial loopback plugs (SLB)
- Custom made RJ-45 Ethernet loopback plug (ELB)

SLB Serial Loopback

Signal wiring on custom made SLB loopback plug:

- Wire RTS to CTS (1 to 8)
- Wire DSR to DCD to DTR (2 to 3 to 7)
- Wire RXD to TXD (4 to 5)

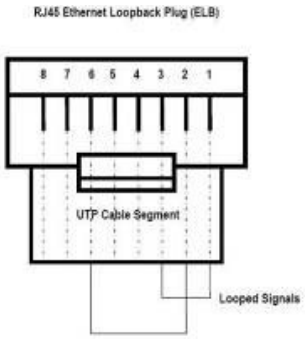


The RJ-45 Serial Modular Jack pinout is:

1	RTS
2	DSR
3	DCD
4	RXD
5	TXD
6	GND
7	DTR
8	CTS

ELB Ethernet Loopback

Signal Wiring on Custom made loopback plug:



- Wire TXD+ to RXD+ (1 to 3)
- Wire TXD- to RXD- (2 to 6)

The RJ-45 Ethernet modular jack pinout is:

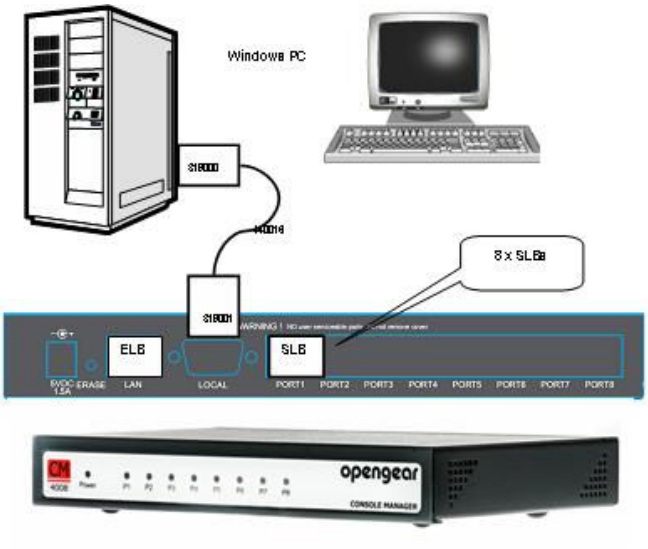
1	TXD+
2	TXD-
3	RXD+
4	NC
5	NC
6	RXD-
7	NC
8	NC

Test Procedure

- Power up the IMG/IM/CM4000 and you should observe the LEDs P1 through P8 light up in sequence
- Configure the serial connection of the “terminal” device/program you are using to 9600bps, 8 data bits, no parity and one stop bit
- Plug a serial cable between the IMG/IM/CM4000 local DB-9 port and terminal device. If you are using “HyperTerminal” or a similar program running on a Windows PC as the terminal device, then the cable is made up from a Cat5 UTP (440016) cable and two DB-9 to RJ-45 adapters (319000 and 319001)
- Log on to the IMG/IM/CM4000 by pressing ‘return’ a few times. The IMG/IM/CM4000 will request a username and password. The username is ‘root’ and the password is ‘default’. You should now see the command line prompt which is a hash (#)

For CM4008:

- Install the ELB on the Ethernet RJ45 socket and an SLB plug onto each serial RJ-45 sockets



- To invoke the inbuilt loopback diagnostics:

  Type in *loopback –e eth0 /dev/port0[1-8]*
  Then press '*return*'

The screen will show 8 columns for serial loopback and one for Ethernet.

1	2	3	4	5	6	7	8	E	
-	-	-	-	-	-	-	-	-	*(- is not looped)*
L	L	L	L	L	L	L	L	L	*(L is looped)*
S	S	S	S	S	S	S	S	S	*(S is too little data received)*
C	C	C	C	C	C	C	C	C	*(C is corrupt data received)*
D	D	D	D	D	D	D	D	D	*(DTR set but not sensed)*
R	R	R	R	R	R	R	R	R	*(RTS set but not sensed)*

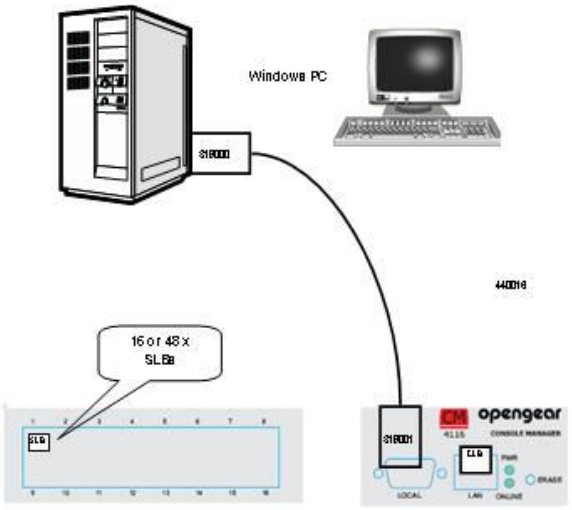
This will test port 1 through 8 and will repeat indefinitely.

The test can be terminated by pressing Ctrl C.

A successful test must have 'L' active in each column.

For CM4116/ CM4148:

- Install the ELB on the Ethernet RJ45 socket and an SLB plug onto each serial RJ-45 sockets



- To invoke the inbuilt loopback diagnostics:

  Type in *loopback –e eth0 /dev/port0[1-9]*
  Then press '*return*'

The screen will show 9 columns for serial loopback and one for Ethernet.

1	2	3	4	5	6	7	8	9	E	
-	-	-	-	-	-	-	-	-	-	*(- is not looped)*
L	L	L	L	L	L	L	L	L	L	*(L is looped)*
S	S	S	S	S	S	S	S	S	S	*(S is too little data received)*
C	C	C	C	C	C	C	C	C	C	*(C is corrupt data received)*
D	D	D	D	D	D	D	D	D	D	*(DTR set but not sensed)*
R	R	R	R	R	R	R	R	R	R	*(RTS set but not sensed)*

This will test port 1 through 9.To test ports 10 through 16 on the CM4116 you need to type -

loopback –e eth0 /dev/port1[0-6]

The screen will then show 7 columns for ports 10 through 16 and one for Ethernet.

As the CM4148 has 48 ports you need to test ports, 1-9, 10-19, 20-29, 30-39, 40-48 in separate blocks.

For ports 10 through 19, type in –

loopback –e eth0 /dev/port1[0-9]

For ports 20 through 29, type in –

loopback –e eth0 /dev/port2[0-9]

For ports 30 through 39, type in –

loopback –e eth0 /dev/port3[0-9]

For ports 40 through 48, type in –

loopback –e eth0 /dev/port4[0-8]

The test will repeat indefinitely.

The test can be terminated by pressing Ctrl C.

A successful test must have ‘L’ active in each column.

Appendix F Terminology

TERM	MEANING
Authentication	Authentication is the technique by which a process verifies that its communication partner is who it is supposed to be and not an imposter. Authentication confirms that data is sent to the intended recipient and assures the recipient that the data originated from the expected sender and has not been altered on route
BIOS	Basic Input/Output System is the built-in software in a computer that are executed on start up (boot) and that determine what the computer can do without accessing programs from a disk. On PCs, the BIOS contains all the code required to control the keyboard, display screen, disk drives, serial communications, and a number of miscellaneous functions
Bonding	Ethernet Bonding or Failover is the ability to detect communication failure transparently, and switch from one LAN connection to another.
BOOTP	Bootstrap Protocol. A protocol that allows a network user to automatically receive an IP address and have an operating system boot without user interaction. BOOTP is the basis for the more advanced DHCP
Certificates	A digitally signed statement that contains information about an entity and the entity's public key, thus binding these two pieces of information together. A certificate is issued by a trusted organization (or entity) called a Certification Authority (CA) after the CA has verified that the entity is who it says it is.
Certificate Authority	A Certificate Authority is a trusted third party, which certifies public key's to truly belong to their claimed owners. It is a key part of any Public Key Infrastructure, since it allows users to trust that a given public key is the one they wish to use, either to send a private message to its owner or to verify the signature on a message sent by that owner.
Certificate Revocation List	A list of certificates that have been revoked by the CA before they expired. This may be necessary if the private key certificate has been compromised or if the holder of the certificate is to be denied the ability to establish a connection to the IMG/IM/CM4000.
CHAP	Challenge-Handshake Authentication Protocol (CHAP) is used to verify a user's name and password for PPP Internet connections. It is more secure

	than PAP, the other main authentication protocol.
DHCP	Dynamic Host Configuration Protocol. A communications protocol that assigns IP addresses to computers when they are connected to the network.
DNS	Domain Name System that allocates Internet domain names and translates them into IP addresses. A domain name is a meaningful and easy to remember name for an IP address.
DUN	Dial Up Networking
Encryption	The technique for converting a readable message (plaintext) into apparently random material (ciphertext) which cannot be read if intercepted. The proper decryption key is required to read the message.
Ethernet	A physical layer protocol based upon IEEE standards
Firewall	A network gateway device that protects a private network from users on other networks. A firewall is usually installed to allow users on an intranet access to the public Internet without allowing public Internet users access to the intranet.
Gateway	A machine that provides a route (or pathway) to the outside world.
Hub	A network device that allows more than one computer to be connected as a LAN, usually using UTP cabling.
Internet	A worldwide system of computer networks - a public, cooperative, and self-sustaining network of networks accessible to hundreds of millions of people worldwide. The Internet is technically distinguished because it uses the TCP/IP set of protocols.
Intranet	A private TCP/IP network within an enterprise.
IPMI	Intelligent Platform Management Interface (IPMI) is a remote hardware health monitoring and management system that defines interfaces for use in monitoring the physical health of servers, such as temperature, voltage, fans, power supplies and chassis. It was developed by Dell, HP, Intel and NEC, but has now been adopted by more than 150 server technology and ships with over 70% of servers. Servers with IPMI functionality let network managers access and monitor server hardware, and diagnose and restore a frozen server to normal operation. IPMI defines the protocols for interfacing with a service processor embedded into a server platform.
Key lifetimes	The length of time before keys are renegotiated
LAN	Local Area Network
LDAP	The Lightweight Directory Access Protocol (LDAP) is based on the X.500

	standard, but significantly simpler and more readily adapted to meet custom needs. The core LDAP specifications are all defined in RFCs. LDAP is a protocol used to access information stored in an LDAP server.
LED	Light-Emitting Diode
MAC address	Every piece of Ethernet hardware has a unique number assigned to it called it's MAC address. Ethernet is used locally to connect the IMG/IM/CM4000 to the Internet, and it may share the local network with many other appliances. The MAC address is used by the local Internet router in order to direct IMG/IM/CM4000 traffic to it rather than somebody else in the local area. It is a 48-bit number usually written as a series of 6 hexadecimal octets, *e.g.* 00:d0:cf:00:5b:da. A IMG/IM/CM4000 has a MAC address listed on a label underneath the device.
MSCHAP	Microsoft Challenge Handshake Authentication Protocol (MSCHAP) is authentication for PPP connections between a computer using a Microsoft Windows operating system and a network access server. It is more secure than PAP or CHAP, and is the only option that also supports data encryption.
NAT	Network Address Translation. The translation of an IP address used on one network to an IP address on another network. Masquerading is one particular form of NAT.
Net mask	The way that computers know which part of a TCP/IP address refers to the network, and which part refers to the host range.
NFS	Network File System is a protocol that allows file sharing across a network. Users can view, store, and update files on a remote computer.
NTP	Network Time Protocol (NTP) used to synchronize clock times in a network of computers
OUT OF BAND	Out-of-Band (OoB) management is any management done over channels and interfaces that are separate from those used for user/customer data. Examples would include a serial console interface or a network interface connected to a dedicated management network that is not used to carry customer traffic, or to a BMC/service processor. Any management done over the same channels and interfaces used for user/customer data is In Band.
PAP	Password Authentication Protocol (PAP) is the usual method of user authentication used on the internet: sending a username and password to a server where they are compared with a table of authorized users. Whilst most common, PAP is the least secure of the authentication options.
PPP	Point-to-Point Protocol. A networking protocol for establishing simple links between two peers.

RADIUS	The Remote Authentication Dial-In User Service (RADIUS) protocol was developed by Livingston Enterprises as an access server authentication and accounting protocol. The RADIUS server can support a variety of methods to authenticate a user. When it is provided with the username and original password given by the user, it can support PPP, PAP or CHAP, UNIX login, and other authentication mechanisms.
Router	A network device that moves packets of data. A router differs from hubs and switches because it is "intelligent" and can route packets to their final destination.
SMASH	Systems Management Architecture for Server Hardware is a standards-based protocols aimed at increasing productivity of the management of a data center. The SMASH Command Line Protocol (SMASH CLP) specification provides an intuitive interface to heterogeneous servers independent of machine state, operating system or OS state, system topology or access method. It is a standard method for local and remote management of server hardware using out-of-band communication
SMTP	Simple Mail Transfer Protocol. IMG/IM/CM4000 includes, SMTPclient, a minimal SMTP client that takes an email message body and passes it on to a SMTP server (default is the MTA on the local host).
SOL	Serial Over LAN (SOL) enables servers to transparently redirect the serial character stream from the baseboard universal asynchronous receiver/transmitter (UART) to and from the remote-client system over a LAN. With SOL support and BIOS redirection (to serial) remote managers can view the BIOS/POST output during power on, and reconfigured.
SSH	Secure Shell is secure transport protocol based on public-key cryptography.
SSL	Secure Sockets Layer is a protocol that provides authentication and encryption services between a web server and a web browser.
TACACS+	The Terminal Access Controller Access Control System (TACACS+) security protocol is a more recent protocol developed by Cisco. It provides detailed accounting information and flexible administrative control over the authentication and authorization processes. TACACS+ allows for a single access control server (the TACACS+ daemon) to provide authentication, authorization, and accounting services independently. Each service can be tied into its own database to take advantage of other services available on that server or on the network, depending on the capabilities of the daemon. There is a draft RFC detailing this protocol.
TCP/IP	Transmission Control Protocol/Internet Protocol. The basic protocol for Internet communication.
TCP/IP address	Fundamental Internet addressing method that uses the form

	nnn.nnn.nnn.nnn.
Telnet	Telnet is a terminal protocol that provides an easy-to-use method of creating terminal connections to a network.
UTC	Coordinated Universal Time.
UTP	Unshielded Twisted Pair cabling. A type of Ethernet cable that can operate up to 100Mb/s. Also known as Category 5 or CAT 5.
VNC	Virtual Network Computing (VNC) is a desktop protocol to remotely control another computer. It transmits the keyboard presses and mouse clicks from one computer to another relaying the screen updates back in the other direction, over a network.
WAN	Wide Area Network
WINS	Windows Internet Naming Service that manages the association of workstation names and locations with IP addresses

For further technology definitions refer:

http://linux-documentation.com/en/documentation/linux-dictionary/index.html or

http://en.wikipedia.org/

Appendix G End User License Agreement

READ BEFORE USING THE ACCOMPANYING SOFTWARE

YOU SHOULD CAREFULLY READ THE FOLLOWING TERMS AND CONDITIONS BEFORE USING THE ACCOMPANYING SOFTWARE, THE USE OF WHICH IS LICENSED FOR USE ONLY AS SET FORTH BELOW. IF YOU DO NOT AGREE TO THE TERMS AND CONDITIONS OF THIS AGREEMENT, DO NOT USE THE SOFTWARE. IF YOU USE ANY PART OF THE SOFTWARE, SUCH USE WILL INDICATE THAT YOU ACCEPT THESE TERMS.

You have acquired a product that includes Opengear ("Opengear") proprietary software and/or proprietary software licensed to Opengear. This Opengear End User License Agreement ("EULA") is a legal agreement between you (either an individual or a single entity) and Opengear for the installed software product of Opengear origin, as well as associated media, printed materials, and "online" or electronic documentation ("Software"). By installing, copying, downloading, accessing, or otherwise using the Software, you agree to be bound by the terms of this EULA. If you do not agree to the terms of this EULA, Opengear is not willing to license the Software to you. In such event, do not use or install the Software. If you have purchased the Software, promptly return the Software and all accompanying materials with proof of purchase for a refund.

Products with separate end user license agreements that may be provided along with the Software are licensed to you under the terms of those separate end user license agreements.

LICENSE GRANT. Subject to the terms and conditions of this EULA, Opengear grants you a nonexclusive right and license to install and use the Software on a single CPU, provided that, (1) you may not rent, lease, sell, sublicense or lend the Software; (2) you may not reverse engineer, decompile, disassemble or modify the Software, except and only to the extent that such activity is expressly permitted by applicable law notwithstanding this limitation; and (3) you may not transfer rights under this EULA unless such transfer is part of a permanent sale or transfer of the Product, you transfer at the same time all copies of the Software to the same party or destroy such materials not transferred, and the recipient agrees to this EULA.

No license is granted in any of the Software's proprietary source code. This license does not grant you any rights to patents, copyright, trade secrets, trademarks or any other rights with respect to the Software.

You may make a reasonable number of copies of the electronic documentation accompanying the Software for each Software license you acquire, provided that, you must reproduce and include all copyright notices and any other proprietary rights notices appearing on the electronic documentation. Opengear reserves all rights not expressly granted herein.

INTELLECTUAL PROPERTY RIGHTS. The Software is protected by copyright laws, international copyright treaties, and other intellectual property laws and treaties. Opengear and

its suppliers retain all ownership of, and intellectual property rights in (including copyright), the Software components and all copies thereof, provided however, that certain components of the Software are components licensed under the GNU General Public License (version 2), which Opengear supports. You may obtain a copy of the GNU General Public License at http:/www.fsf.org/copyleft/gpl.html. Opengear will provide source code for any of the components of the Software licensed under the GNU General Public License upon request.

EXPORT RESTRICTIONS. You agree that you will not export or re-export the Software, any part thereof, or any process or service that is the direct product of the Software in violation of any applicable laws or regulations of the United States or the country in which you obtained them.

U.S. GOVERNMENT RESTRICTED RIGHTS. The Software and related documentation are provided with Restricted Rights. Use, duplication, or disclosure by the Government is subject to restrictions set forth in subparagraph (c) (1) (ii) of the Rights in Technical Data and Computer Software clause at DFARS 252.227-7013 or subparagraphs (c) (1) and (2) of the Commercial Computer Software – Restricted Rights at 48 C.F.R. 52.227-19, as applicable, or any successor regulations.

TERM AND TERMINATION. This EULA is effective until terminated. The EULA terminates immediately if you fail to comply with any term or condition. In such an event, you must destroy all copies of the Software. You may also terminate this EULA at any time by destroying the Software.

GOVERNING LAW AND ATTORNEY'S FEES. This EULA is governed by the laws of the State of Utah, USA, excluding its conflict of law rules. You agree that the United Nations Convention on Contracts for the International Sale of Goods is hereby excluded in its entirety and does not apply to this EULA. If you acquired this Software in a country outside of the United States, that country's laws may apply. In any action or suit to enforce any right or remedy under this EULA or to interpret any provision of this EULA, the prevailing party will be entitled to recover its costs, including reasonable attorneys' fees.

ENTIRE AGREEMENT. This EULA constitutes the entire agreement between you and Opengear with respect to the Software, and supersedes all other agreements or representations, whether written or oral. The terms of this EULA can only be modified by express written consent of both parties. If any part of this EULA is held to be unenforceable as written, it will be enforced to the maximum extent allowed by applicable law, and will not affect the enforceability of any other part.

Should you have any questions concerning this EULA, or if you desire to contact Opengear for any reason, please contact the Opengear representative serving your company.

THE FOLLOWING DISCLAIMER OF WARRANTY AND LIMITATION OF LIABILITY IS INCORPORATED INTO THIS EULA BY REFERENCE. THE SOFTWARE IS NOT FAULT TOLERANT. YOU HAVE INDEPENDENTLY DETERMINED HOW TO USE THE SOFTWARE IN THE DEVICE, AND OPENGEAR HAS RELIED UPON YOU TO CONDUCT SUFFICIENT TESTING TO DETERMINE THAT THE SOFTWARE IS SUITABLE FOR SUCH USE.

LIMITED WARRANTY Opengear warrants the media containing the Software for a period of ninety (90) days from the date of original purchase from Opengear or its authorized retailer.

Proof of date of purchase will be required. Any updates to the Software provided by Opengear (which may be provided by Opengear at its sole discretion) shall be governed by the terms of this EULA. In the event the product fails to perform as warranted, Opengear's sole obligation shall be, at Opengear's discretion, to refund the purchase price paid by you for the Software on the defective media, or to replace the Software on new media. Opengear makes no warranty or representation that its Software will meet your requirements, will work in combination with any hardware or application software products provided by third parties, that the operation of the software products will be uninterrupted or error free, or that all defects in the Software will be corrected.

OPENGEAR DISCLAIMS ANY AND ALL OTHER WARRANTIES, WHETHER EXPRESS OR IMPLIED, INCLUDING WITHOUT LIMITATION, ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. OTHER THAN AS STATED HEREIN, THE ENTIRE RISK AS TO SATISFACTORY QUALITY, PERFORMANCE, ACCURACY, AND EFFORT IS WITH YOU. ALSO, THERE IS NO WARRANTY AGAINST INTERFERENCE WITH YOUR ENJOYMENT OF THE SOFTWARE OR AGAINST INFRINGEMENT. IF YOU HAVE RECEIVED ANY WARRANTIES REGARDING THE DEVICE OR THE SOFTWARE, THOSE WARRANTIES DO NOT ORIGINATE FROM, AND ARE NOT BINDING ON, OPENGEAR.

NO LIABILITY FOR CERTAIN DAMAGES. EXCEPT AS PROHIBITED BY LAW, OPENGEAR SHALL HAVE NO LIABILITY FOR COSTS, LOSS, DAMAGES OR LOST OPPORTUNITY OF ANY TYPE WHATSOEVER, INCLUDING BUT NOT LIMITED TO, LOST OR ANTICIPATED PROFITS, LOSS OF USE, LOSS OF DATA, OR ANY INCIDENTAL, EXEMPLARY SPECIAL OR CONSEQUENTIAL DAMAGES, WHETHER UNDER CONTRACT, TORT, WARRANTY OR OTHERWISE ARISING FROM OR IN CONNECTION WITH THIS EULA OR THE USE OR PERFORMANCE OF THE SOFTWARE. IN NO EVENT SHALL OPENGEAR BE LIABLE FOR ANY AMOUNT IN EXCESS OF THE LICENSE FEE PAID TO OPENGEAR UNDER THIS EULA. SOME STATES AND COUNTRIES DO NOT ALLOW THE LIMITATION OR EXCLUSION OF LIABILITY FOR INCIDENTAL OR CONSEQUENTIAL DAMAGES, SO THIS LIMITATION MAY NOT APPLY TO YOU.

Appendix H Service and Warranty

STANDARD WARRANTY

Opengear, Inc., its parent, affiliates and subsidiaries, (collectively, "Opengear") warrant your Opengear product to be in good working order and to be free from defects in workmanship and material (except in those cases where the materials are supplied by the Purchaser) under normal and proper use and service for the period of four (4) years from the date of original purchase from an Authorized Opengear reseller (for CM4116, CM4148 and all IM/IMG42xx products) and one (1) year from the date of original purchase from an Authorized Opengear reseller for all other product. In the event that this product fails to meet this warranty within the applicable warranty period, and provided that Opengear confirms the specified defects, Purchaser's sole remedy is to have Opengear, in Opengear's sole discretion, repair or replace such product at the place of manufacture, at no additional charge other than the cost of freight of the defective product to and from the Purchaser. Repair parts and replacement products will be provided on an exchange basis and will be either new or reconditioned. Opengear will retain, as its property, all replaced parts and products. Notwithstanding the foregoing, this hardware warranty does not include service to replace or repair damage to the product resulting from accident, disaster, abuse, misuse, electrical stress, negligence, any non- Opengear modification of the product except as provided or explicitly recommended by Opengear, or other cause not arising out of defects in material or workmanship. This hardware warranty also does not include service to replace or repair damage to the product if the serial number or seal or any part thereof has been altered, defaced or removed. If Opengear does not find the product to be defective, the Purchaser will be invoiced for said inspection and testing at Opengear's then current rates, regardless of whether the product is under warranty.

RMA RETURN PROCEDURE

If this product requires service during the applicable warranty period, a Return Materials Authorization (RMA) number must first be obtained from Opengear. Product that is returned to Opengear for service or repair without an RMA number will be returned to the sender unexamined. Product should be returned, freight prepaid, in its original or equivalent packaging, to:

Opengear Service Center
Suite A, 630 West 9560 South
Sandy, Utah 84070

Proof of purchase date must accompany the returned product and the Purchaser shall agree to insure the product or assume the risk of loss of damage in transit. Contact Opengear by emailing support@opengear.com for further information.

TECHNICAL SUPPORT

Purchaser is entitled to thirty (30) days free telephone support (USA ONLY) and twelve (12) months free e-mail support (world wide) from date of purchase provided that the Purchaser first register their product(s) with Opengear by filling in the on-line form http://www.opengear.com/registration.html. Telephone and e-mail support is available from 9:00 AM to 5:00 PM, Mountain Time.

Opengear's standard warranty includes free access to Opengear's Knowledge Base as well as any application notes, white papers and other on-line resources that may become available from time to time.

Opengear reserves the right to discontinue all support for products that are no longer covered by warranty.

LIMITATION OF LIABILITY

No action, regardless of form, arising from this warranty may be brought by either party more than two (2) years after the cause of action has occurred. Purchaser expressly agrees that Opengear's liability, if any, shall be limited solely to the replacement or repair of the product in accordance with the warranties specifically and expressly set forth herein. The remedies of the Purchaser are the exclusive and sole remedies available, and, in the event of a breach or repudiation of any provision of this agreement by Opengear, the Purchaser shall not be entitled to receive any incidental damages as that term is defined in Section 2-715 of the Uniform Commercial Code. Opengear waives the benefit of any rule that disclaimer of warranty shall be construed against Opengear and agrees that such disclaimers herein shall be construed liberally in favor of Opengear.

THE FOREGOING WARRANTIES ARE THE SOLE ANDEXCLUSIVE WARRANTIES GIVEN IN CONNECTION WITH THE PRODUCT AND THE HARDWARE. OPENGEAR DISCLAIMS ALL OTHER WARRANTIES, EXPRESS OR IMPLIED, INCLUDING WITHOUT LIMITATION, ANY WARRANTIES AS TO THE SUITABILITY OR MERCHANTABILITY OR FITNESS FOR ANY PARTICULAR PURPOSE AND NONINFRINGEMENT OF THIRD PARTY RIGHTS. OPENGEAR DOES NOT PROMISE THAT THE PRODUCT IS ERROR-FREE OR WILL OPERATE WITHOUT INTERRUPTION. IN NO EVENT SHALL OPENGEAR BE LIABLE FOR ANY LOST OR ANTICIPATED PROFITS, OR ANY INCIDENTAL, EXEMPLARY, SPECIAL OR CONSEQUENTIAL DAMAGES, REGARDLESS OF WHETHER OPENGEAR WAS ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.